Postverlagsort Berlin

MATHEMATISCHE ZEITSCHRIFT

UNTER STÄNDIGER MITWIRKUNG VON

E. KAMKE
TÜBINGEN

R. NEVANLINNA
HELSINKI

F. K. SCHMIDT
HEIDELBERG

HERAUSGEGEBEN VON

H. WIELANDT
TÜBINGEN

WISSENSCHAFTLICHER BEIRAT

W. BLASCHKE A. E. INGHAM H. KNESER
W. MAGNUS O. PERRON G. PICKERT

74. BAND, 1. HEFT

(ABGESCHLOSSEN AM 15. AUGUST 1960)

BERLIN · GÖTTINGEN · HEIDELBERG
SPRINGER-VERLAG
1960

Z.

Die **MATHEMATISCHE ZEITSCHRIFT**

wurde im Jahre 1918 von *L. Lichtenstein* unter der Mitwirkung von *K. Knopp*, *E. Schmidt* und *I. Schur* gegründet und herausgegeben. Nach dem Tode Lichtensteins übernahm *K. Knopp* 1933 die Herausgabe. Die Schriftleitung ergänzte sich 1933 durch *E. Kamke* und *F. K. Schmidt*, 1936 durch *R. Nevanlinna* und 1950 durch *H. Wielandt*, der 1952 die Herausgabe übernahm.

Die Zeitschrift erscheint nach Maßgabe des eingehenden Materials. Der Preis des Bandes beträgt DM 96.—.

Die Mathematische Zeitschrift ist durch jede Buchhandlung zu beziehen.

Die Mathematische Zeitschrift dient der Pflege der reinen Mathematik, doch werden auch Beiträge aus den Gebieten der theoretischen Physik und Astronomie Aufnahme finden, soweit sie mathematisch von Interesse sind. Besprechungen, Aufgaben u. dgl. werden nicht zugelassen.

Grundsätzlich dürfen nur Arbeiten eingereicht werden, die vorher weder im Inland noch im Ausland veröffentlicht worden sind. Der Autor verpflichtet sich, sie auch nachträglich nicht an anderer Stelle zu publizieren. Mit der Annahme des Manuskriptes und seiner Veröffentlichung durch den Verlag geht das Verlagsrecht für alle Sprachen und Länder einschließlich des Rechts der fotomechanischen Wiedergabe oder einer sonstigen Vervielfältigung an den Verlag über. Jedoch wird gewerblichen Unternehmen für den innerbetrieblichen Gebrauch nach Maßgabe des zwischen dem Börsenverein des Deutschen Buchhandels e. V. und dem Bundesverband der Deutschen Industrie abgeschlossenen Rahmenabkommens die Anfertigung einer fotomechanischen Vervielfältigung gestattet. Wenn für diese Zeitschrift kein Pauschalabkommen mit dem Verlag vereinbart worden ist, ist eine Wertmarke im Betrage von DM 0.30 pro Seite zu verwenden. *Der Verlag läßt diese Beträge den Autorenverbänden zufließen.*

Die Mitarbeiter erhalten von ihren Arbeiten 75 Sonderdrucke unentgeltlich.

Manuskriptsendungen sind zu richten an die Mitglieder der unterzeichneten Redaktion. Die Herren Mitarbeiter werden im Interesse einer raschen Drucklegung gebeten, die Arbeiten in gut lesbarer Niederschrift einzureichen. Für den Text ist, wenn irgend möglich, Maschinenschrift, für die mathematischen Formeln jedoch nur Handschrift zu verwenden. Etwaige Abbildungen sind auf einem besonderen Blatt zu zeichnen. Die in den Formeln etwa vorkommenden griechischen oder deutschen Buchstaben (Fraktur) sowie andere der Gefahr von Verwechselungen ausgesetzte Zeichen, z. B. die Landauschen Symbole o und O, sind stets besonders (etwa mit verschiedenfarbigen Stiften) zu kennzeichnen. Die Fußnoten sind fortlaufend zu numerieren, bei Zitaten Erscheinungsjahr und Seitenzahlen anzugeben.

Wenn zu einer bereits gedruckten Arbeit eine Berichtigung nötig wird, wollen die Herren Verfasser dem Herausgeber hiervon unverzüglich Mitteilung machen. Die Berichtigungen sollen dann am Schlusse eines Bandes gesammelt aufgenommen werden.

REDAKTION DER MATHEMATISCHEN ZEITSCHRIFT:

E. Kamke, Tübingen, Frischlinstraße 27,

R. Nevanlinna, Helsinki (Finnland), Math. Inst. d. Universität, Portania.

F. K. Schmidt, Heidelberg, Mathematisches Institut,

H. Wielandt, Tübingen, Ob dem Viehweidle 21 b.

Springer-Verlag OHG — Berlin-Wilmersdorf, Heidelberger Platz 3 — Heidelberg, Neuenheimer Landstraße 28/30. — Göttingen, Weender Straße 60.

---

74. Band **Inhalt** 1. Heft

Seite

Feit, W., M. Hall jr. and J. G. Thompson, Finite groups in which the centralizer of any non-identity element is nilpotent 1

Fröhlich, A., Discriminants of algebraic number fields 18

Fröhlich, A., Ideals in an extension field as modules over the algebraic integers in a finite number field 29

Menzel, W., Über den Untergruppenverband einer Abelschen Operatorgruppe. Teil I: m-Verbände 39

Menzel, W., Über den Untergruppenverband einer Abelschen Operatorgruppe. Teil II: Distributive und m-Verbände von Untergruppen einer Abelschen Operatorgruppe 52

Cohen, E., Arithmetical functions associated with the unitary divisors of an integer 66

Krull, W., Über die Endomorphismen von total geordneten Archimedischen Abelschen Gruppen 81

FEIT, W., M. HALL jr. and J. G. THOMPSON
Math. Zeitschr. 74, 1—17 (1960)

Finite groups in which the centralizer of any non-identity element is nilpotent

By

WALTER FEIT[1]), MARSHALL HALL jr., and JOHN G. THOMPSON

Introduction

SUZUKI [6] showed that a non-solvable finite group in which the centralizer of any non-identity element is abelian is necessarily of even order.

In another vein, G. HIGMAN [5] has studied groups in which every element has order a power of a prime, the prime being allowed to vary from element to element. Such groups have the property that the centralizer of any non-identity element is a p-group for some prime p.

Theorem A, proved here, generalizes SUZUKI's result by replacing "abelian" with "nilpotent". At the same time, Theorem A gives information about groups in which every element is of prime-power order.

I. Statement of Theorem A, and group-theoretic lemmas

THEOREM A. *If G is a finite non-solvable group, and if the centralizer of any non-identity element of G is nilpotent, then G is of even order.*

A finite group X in which $C_X(x)$ is nilpotent for x in X, $x \neq 1$, will be called a CN-group. (X) denotes the order of X, as does $[X:1]$. All groups referred to are assumed finite.

LEMMA 1.1. *If X is a group, A is a group of automorphisms of X, and each non-identity element of A is a fixed-point-free automorphism of X, and T is an A-invariant normal subgroup of X, then the non-identity elements of A induce fixed-point-free automorphisms of X/T.*

PROOF. Let $\sigma \in A$, $\sigma \neq 1$. Since $\sigma(x)\,x^{-1} = 1$ implies $x = 1$, and $\sigma(x)\,x^{-1} = \sigma(y)\,y^{-1}$ implies $\sigma(y^{-1}x) = y^{-1}x$ so that $x = y$, it follows that each element u of X is represented uniquely as $\sigma(x)\,x^{-1} = u$ for some x in X. If σ fixes the coset yT, then $\sigma(y)\,y^{-1} \in T$. Since T is assumed A-invariant, $\sigma(y)\,y^{-1} = \sigma(t)\,t^{-1}$ for some $t \in T$. Hence, $y = t \in T$, so that σ is fixed-point-free on X/T.

LEMMA 1.2. *If a q-group Q, q an odd prime, normalizes a group N, and if each non-identity element of Q induces a fixed-point-free automorphism of N, then Q is cyclic.*

PROOF. [1, pp. 334—335].

[1]) The work of the first author was supported by the Office of Ordnance Research, U.S.Army.

LEMMA 1.3. *In a CN-group X, if p_1 and p_2 are distinct primes, P_i is a Sylow p_i-subgroup of X, and $x_i \in P_i$, $x_i \neq 1$, $i=1, 2$, satisfy $x_1 x_2 = x_2 x_1$, then P_1 and P_2 permute elementwise.*

PROOF. $\{x_2, Z(P_1)\} \subseteq C_X(x_1)$ is nilpotent, whence x_2 and $Z(P_1)$ permute elementwise. Hence, $\{x_2, P_1\} \subseteq C_X(Z(P_1))$ is nilpotent, so x_2 and P_1 permute elementwise. Then also $\{P_1, Z(P_2)\} \subseteq C_X(x_2)$, so P_1 and $Z(P_2)$ permute elementwise. Finally, $\{P_1, P_2\} \subseteq C_X(Z(P_2))$ so that P_1 and P_2 permute elementwise.

We write $Z_1(P) = Z(P)$, $Z_2(P)$, $Z_3(P)$ ... for the terms of the ascending central series of P.

LEMMA 1.4. *If P is a non-cyclic p-group, p odd, then $Z_2(P)$ is non-cyclic.*

PROOF. If $Z_1(P) = Z(P)$ is non-cyclic, then since $Z_1(P) \subseteq Z_2(P)$, the lemma follows. Hence, we can suppose that $Z_1(P)$ is cyclic. Since P is assumed non-cyclic, P is non-abelian. We can further suppose that $Z_2(P)$ is cyclic, and that P is a group of least possible order violating the lemma.

If $Z_3(P)$ were cyclic, then since

$$Z_2(P/Z(P)) = Z_3(P)/Z(P),$$

we would conclude from the minimal nature of P that $P/Z(P)$ was cyclic, so that P would be abelian. Hence, we can assume that $Z_3(P)$ is non-cyclic. If

$$x \in Z_3(P), \quad \text{and} \quad x^p = 1, \tag{1.1}$$

we will show that $[x, y, z] = 1$ for all $y, z \in P$, so that $x \in Z_2(P)$. Set $u = [x, y]$, so that

$$y^{-1} x y = x \cdot u, \tag{1.2}$$

and $u \in Z_2(P)$, since $x \in Z_3(P)$. Since $u \in Z_2(P)$,

$$[u, x, x] = 1. \tag{1.3}$$

Using (1.3) and the identity

$$[a, b\,c] = [a, c]\,[a, b]\,[a, b, c],$$

which holds in the free group, we conclude by induction that

$$[u, x^n] = [u, x]^n, \tag{1.4}$$

for all positive integers n. Taking $n = p$, by (1.1) and (1.4) we have

$$[u, x]^p = 1. \tag{1.5}$$

Using (1.3) and (1.4), we conclude by induction that

$$(x\,u)^n = x^n\,u^n\,[u, x]^{\frac{n(n-1)}{2}},$$

for all positive integers n. Taking $n = p$, using (1.1) and (1.2), we conclude

$$1 = u^p\,[u, x]^{\frac{p(p-1)}{2}}. \tag{1.6}$$

Since p is odd, (1.5) and (1.6) yield

$$1 = u^p.$$

Since $u \in Z_2(P)$, and $Z_2(P)$ is cyclic, we conclude that $u \in Z(P)$, so that $[u, z] = [x, y, z] = 1$, as desired. We have shown that all elements of order p in $Z_3(P)$ are contained in $Z_2(P)$, and hence that $Z_3(P)$ contains only one subgroup of order p. By [1, p. 131], $Z_3(P)$ is cyclic. This contradiction completes the proof of this lemma.

LEMMA 1.5. *If Y is a CN-group, and A is a solvable normal subgroup of Y, then Y/A is a CN-group.*

PROOF. We proceed by double induction on (Y) and (A), assuming the lemma true for all Y_1 and A_1, A_1 a solvable normal subgroup of the CN-group Y_1, such that either $(Y_1) < (Y)$, or $(Y_1) = (Y)$ and $(A_1) < (A)$.

CASE 1. A is an elementary abelian p-group. We must show that if yA is a non-identity element of Y/A, then $C_{Y/A}(yA)$ is nilpotent. If C is the inverse image in Y of $C_{Y/A}(yA)$ and if $C < Y$, then the pair C, A is less than the pair Y, A in the ordering, so that $C/A = C_{Y/A}(yA)$ is nilpotent. Hence, we can assume that $C = Y$, and we can assume that yA has prime order q.

SUBCASE 1. $q \neq p$. We can assume in this case that y has order q. The hypothesis that yA is in the center of Y/A is equivalent to the assertion that for every $g \in Y$,

$$g\,y\,g^{-1} = y\,a, \qquad a = a(g) \in A. \tag{1.7}$$

From (1.7) it follows that $y^{-1}Agy = Ag$ for every $g \in Y$. Since the number of elements in the coset Ag is a power of p, and since y is of order $q \neq p$, it follows that y centralizes some element in the coset Ag. Hence, $C_Y(y) \cdot A = Y$, so that $Y/A \cong C_Y(y)/A \cap C_Y(y)$ is nilpotent.

SUBCASE 2. $q = p$. Put $B = \{y, A\}$, so that B is a p-group, and then choose x in Y of prime power order prime to p. Then x fixes the coset yA, and since x has order prime to p, it centralizes some element of yA, say ya. By lemma 1.3, x centralizes A, and hence $A \cap Z(Y_p)$, Y_p being a Sylow p-subgroup of Y. Since $A \lhd Y$, $A \cap Z(Y_p) \neq 1$, and since x was any element of prime power order prime to p, $A \cap Z(Y_p) \subseteq Z(Y)$, so that Y is nilpotent, so also Y/A. This completes the first case.

CASE 2. A is not an elementary abelian p-group. Choose $A_1 \neq 1$, A_1 characteristic in A, so that $A_1 \lhd Y$. By induction, Y/A_1 is a CN-group, by a second induction, $Y/A_1/A/A_1$ is a CN-group isomorphic to Y/A.

LEMMA 1.6. *If Theorem* A *is false, then there is a CN-group T which has the properties:*

1. *T is simple.*
2. *Every proper subgroup of T is solvable.*
3. *T is of odd order.*

PROOF. Let H be any group violating Theorem A, so that H is non-solvable of odd order. Let K be a non-solvable subgroup of H of least possible order, so that every proper subgroup of K is solvable, and let $L \geqq 1$ be the maximal solvable normal subgroup of K. Subgroups of CN-groups are again CN-groups, so K is a CN-group. By lemma 1.5, $T = K/L$ is a CN-group. T is simple since it has no solvable normal subgroups, and all its proper subgroups are solvable.

The remainder of this section is devoted to the study of a CN-group G satisfying the conditions 1, 2, 3 of lemma 1.6.

If the Sylow p-subgroup P of G is not cyclic, we choose $W = W(P)$ as follows: in case $Z(P)$ is not cyclic, we choose $W(P)$ to be any non-cyclic subgroup of $Z(P)$ of order p^2. In case $Z(P)$ is cyclic, we choose $W(P)$ to be any non-cyclic subgroup of $Z_2(P)$ of order p^2 which contains $\Omega_1(Z(P))$, the subgroup of elements of order at most p in $Z(P)$. Since P is not cyclic and since p is odd, $Z_2(P)$ is not cyclic by lemma 1.4, so in this second case, we will be able to find a subgroup $W(P)$ of the desired type. We put

$$V(P_0) = V_G(W; P_0) = \{(W(P))^x \mid (W(P))^x \leqq P_0,\ x \in G\},$$

P_0 being any subgroup of G.

LEMMA 1.7. *If P is a non-cyclic Sylow p-subgroup of G, and $y \in G$ is a p-element which centralizes a subgroup U of $W(P)$ of order p, then*

$$[y, w, w] = 1 \tag{1.8}$$

for every w in $W(P)$.

PROOF. Case 1. $W(P) \leqq Z(P)$. In this case, $U \leqq Z(P)$, so that $C_G(U) \geqq \{P, y\}$ Since $C_G(U)$ is nilpotent, so is $\{P, y\}$. This forces $y \in P$, so $[y, w] = 1$ for all $w \in W$. All the moreso, (1.8) holds.

Case 2. $W(P) \not\leqq Z(P)$. This can only occur because $Z(P)$ is cyclic. In case $U \leqq Z(P)$, we again conclude that $\{y, P\}$ is nilpotent, so that $y \in P$, and (1.8) holds since $W(P) \leqq Z_2(P)$. If $U \not\leqq Z(P)$, then the cyclicity of $Z(P)$ tells us that $C_P(U)$ is of index p in P. Hence $C_P(U) = P \cap C_G(U)$ is either a Sylow p-subgroup of $C_G(U)$ or is of index p in the Sylow p-subgroup P^* of $C_G(U)$. In any case, $C_P(U) \lhd P^*$. Clearly, $Z(P) \leqq C_P(U) < P$, so that $Z(P) \leqq Z(C_P(U))$, and so $W(P) \leqq Z(C_P(U))$, since $\Omega_1(Z(P))$ and U generate $W(P)$. The p-element y lies in the nilpotent group $C_G(U)$, and so in P^*. If $w \in W(P)$, then $[y, w] \in C_P(U)$, since $C_P(U) \lhd P^*$. Hence $[y, w, w] = 1$ since $w \in W(P) \leqq Z(C_P(U))$.

The remainder of this section is devoted to proving Theorem 1.

THEOREM 1. *If P is any Sylow p-subgroup of G, then $P \cap P^x = 1$ or P for each $x \in G$.*

The proof of this theorem will be by contradiction. We leave as an exercise that Theorem 1 holds in case P is abelian, so we confine attention to the non-abelian, and hence non-cyclic, Sylow subgroups of G.

Since Theorem 1 is assumed false, we choose $P^x \neq P$ so that $K = P \cap P^x$ has maximal possible order, so that $1 < K < P$, and we set $N = N_G(K)$. Since

$N \supseteq N_P(K) > K$, and $N \supseteq N_{Px}(K) > K$, by [2, p. 44], it follows from the maximal nature of K that $\{N_P(K), N_{Px}(K)\}$ is not a p-group. Consequently, the Sylow p-subgroups of N are not normal in N, and in particular N is not nilpotent, and more particularly, N is not a p-group. Since $K \neq 1$, $N < G$, so N is solvable. Hence, N satisfies the hypotheses of the next lemma.

LEMMA 1.8. *If S is a solvable CN-group of odd order, if S possesses a non-trivial normal p-subgroup, and if a Sylow p-subgroup S_p of S is not normal in S, then S possesses a normal series*

$$1 < H < K < S,$$

where H is a p-subgroup of S, K/H is a cyclic group of order prime to p, and S/K is a cyclic p-group. Furthermore, if $K = HL$, $H \cap L = 1$, then the non-identity elements of L induce fixed-point-free automorphisms of H, and if $\overline{S} = S/H$, $\overline{K} = K/H$, and $\overline{S}_p = S_p/H$, then the non-identity elements of $\overline{S}_p$ induce fixed-point-free automorphisms of $\overline{K}$.

PROOF. Let H be the maximal normal p-subgroup of S, and let M be the maximal normal p'-subgroup of S. By assumption, $H \neq 1$. Suppose $M \neq 1$. Since H and M are normal subgroups of S, of coprime orders, they permute elementwise. By lemma 1.3, S_p and M permute elementwise. Since $M \neq 1$, $C_S(M)$ is nilpotent, and contains S_p. Since $M \lhd S$, $C_S(M) \lhd S$. Since $C_S(M)$ is nilpotent, S_p is characteristic in $C_S(M)$, so $S_p \lhd S$, contrary to assumption. Hence, $M = 1$.

Since $M = 1$, $H \supseteq C_S(H)$ by [2, p. 5]. By lemma 1.3, elements in S of order prime to p induce fixed-point-free automorphisms of H. It follows now from lemma 1.2 that S_q, a Sylow q-subgroup of S, $q \neq p$, is cyclic. Since S is solvable, given primes q and r, we can find S_q and S_r which are permutable [4]. If $qr \mid (S)$, $q \neq p \neq r \neq q$, then $S_q \cdot S_r$ possesses a subgroup D of order qr, since if $q > r$, then $S_q \lhd S_q \cdot S_r$, both S_q and S_r being cyclic. Since the non-identity elements of D induce fixed-point-free automorphisms of H, D is cyclic [1, pp. 334–335]. (As pointed out elsewhere, BURNSIDE's Theorem V, p. 336, is false. What he actually proved is the assertion made here.) By lemma 1.3, S_q and S_r permute elementwise. It follows immediately that a Sylow complement L of S_p in S, which exists by [4], is cyclic.

Since S/H has no non-trivial normal p-subgroups, and since L is abelian, it follows from [2, p. 5] that

$$LH/H \lhd S/H,$$

so that $LH = K \lhd S$. The remaining assertions of this lemma follow directly from lemmas 1.2, 1.3, and [2, p. 5].

Definition

$\mathscr{H} = [H \mid$ 1. H is a p-subgroup of G.

2. The Sylow p-subgroups of $N_G(H)$ are not normal in $N_G(H)$.

3. $N_G(H)/C_G(H)$ is not a p-group.$]$

By lemma 1.8 and the remark preceding lemma 1.8, $\mathscr{H}$ is not empty. If $H_1, H_2 \in \mathscr{H}$, then $H_1 \leqq H_2$ means

1. $(N_G(H_1)) < (N_G(H_2))$,

or

2. $(N_G(H_1)) = (N_G(H_2))$, and $(H_1) < (H_2)$,

or

3. $H_1 = H_2$.

We see that $\leqq$ is a partial ordering, and that conjugate subgroups are not comparable.

LEMMA 1.9. *If $H \in \mathscr{H}$ is maximal in the ordering $\leqq$, and if P_0 is a Sylow p-subgroup of $N = N_G(H)$, then*

$$V_G(W; P_0) = V_G(W; H).$$

PROOF. By maximality of H in the ordering $\leqq$, H is the maximal normal p-subgroup of N. By lemma 1.8, N has a chief series

$$1 < H < HL < N,$$

where L is cyclic of order prime to p, and P_0/H is cyclic. Suppose $W^x \leqq P_0$. Then $H \cap W^x \neq 1$, since P_0/H is cyclic and W^x is of type (p, p). By lemma 1.7,

$$[Z(H), w, w] = 1, \quad \text{for all } w \in W^x.$$

If we represent N as linear transformations of $\Omega_1(Z(H))$, we have a faithful representation of N/H, by lemma 1.8. By theorem B of HALL and HIGMAN [2, p. 3], W^x is in the kernel, that is, $W^x \leqq H$. This completes the proof of lemma 1.9.

We remark that $V_G(W; P_0) \neq 1$. Namely, if $P_0 \leqq P^y$, then $Z(P^y)$ centralizes H, so that $Z(P^y) \leqq Z(H) \leqq H$, since H contains its centralizer. If $W^y \leqq Z(P)^y$, then $W^y \leqq V_G(W; P_0)$. If $W^y \not\leqq Z(P^y)$, then $Z(P^y)$ is cyclic, and we at least have $Z(P^y) \leqq H$. But then $Z_2(P^y)$ normalizes H, so that $Z_2(P^y) \leqq P_0$ and once again $W^y \leqq V_G(W; P_0)$.

LEMMA 1.10. $V(W; P_0) \in \mathscr{H}$.

PROOF. Since $V(W; P_0) = V(W; H) \lhd N_G(H)$, and $V(W; P_0) \neq 1$, we only need to show that $N_G(V(W; H))/C_G(V(W; H))$ is not a p-group. But this is obvious, since the non-identity elements in the group L of the previous lemma induce fixed-point-free automorphisms of $V(W; H)$.

LEMMA 1.11. *P_0 is a Sylow p-subgroup of G.*

PROOF. Otherwise $(N_G(H)) < (N_G(V_G(W; P_0)))$, and H would not be maximal in the ordering $\leqq$.

LEMMA 1.12. $N_G(H) = N_G(V_G(W; P_0))$.

PROOF. Since $N_G(H) \leqq N_G(V_G(W; P_0))$, maximality of H in the ordering $\leqq$ forces equality.

This sequence of lemmas tells us that if H is maximal in the ordering $\ll$, if $H \lhd P$, $H \in \mathscr{H}$ then,

$$N = N_G(H) = N_G\big(V_G(W; P)\big) = N_G(V),$$

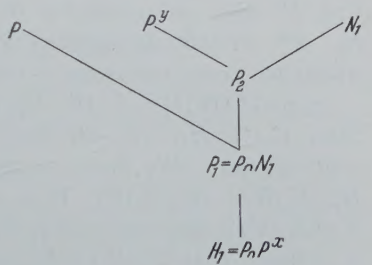
where $V = V_G(W; P)$ is the group selected earlier. Since $P \leqq N$, and $N_N(P) = P$, and since $N_G(V) \geqq N_G(P)$, it follows that

$$N_G(P) = N_N(P) = P,$$

so that P is its own normalizer in G. We denote by H_0 the maximal normal p-subgroup of $N_G(V)$.

LEMMA 1.13. *If* $P^x \neq P$, *then* $P \cap P^x \leqq H_0$.

PROOF. Assume false. Choose P^x so that $P^x \neq P$ and $P \cap P^x = H_1$, is of maximal order subject to the restriction $H_1 \leqq H_0$. Put $N_1 = N_G(H_1)$, and $P_1 = P \cap N_1$, let P_1 be contained in the Sylow p-subgroup P_2 of N_1, and let P_2 be contained in the Sylow p-subgroup P^y of G. The following diagram is explanatory: H_1 is a proper subgroup of P_1, by a fundamental property of p-groups [2, p. 44]. If P_2 were not contained in P, then $P \neq P^y$, and $P^y \cap P \geqq P_2 \cap P = P_1 > H_1 = P^x \cap P$, contrary to our choice of H_1. Hence $P^y = P$, so that $P_1 = P_2$ is a Sylow p-subgroup of N_1.



Also, by the maximal nature of H_1, P_1 is not normal in N_1, so we are in a position to apply lemma 1.8 to N_1.

It is clear that H_1 is the maximal normal p-subgroup of N_1, since the maximal normal p-subgroup of N_1 is contained in P and in at least one other Sylow p-subgroup of G.

As in the proof of lemma 1.9, we conclude that $V_G(W; P_1) = V_G(W; H_1)$. Let the relevant chief series for N_1 be

$$1 < H_1 < H_1 L_1 < N_1,$$

L_1 being cyclic of order prime to p, while $N_1/H_1 L_1 \cong P_1/H_1$ is a cyclic p-group.

Suppose $P_1 < P$. Then $P_1 \lhd P^* \leqq P$, $P_1 < P^*$, for suitable choice of P^*, [2, p. 44], and we find

$$\{P^*, N_1\} \leqq N_G\big(V_G(W; H_1)\big) = N_2,$$

say. The Sylow p-subgroups of N_2 are not normal in N_2, since if they were we would find that the Sylow p-subgroups of N_1 are normal in N_1, which is not the case. Since $V_G(W; H) \neq 1$, application of lemma 1.8 yields a chief series

$$1 < H_2 < H_2 L_2 < N_2$$

of N_2, L_2 being cyclic of order prime to p, and $N_2/H_2 L_2$ being a cyclic p-group. Since L_2 is abelian, and since $L_1 < N_1 < N_2$, we can apply WIELANDT's theorem

on the conjugacy of nilpotent Hall subgroups [7] to conclude that $L_1 \leqq L_2^v$ for suitable $v \in N_2$. Hence, without loss of generality, we suppose that $L_1 \leqq L_2$.

If H_1 were not contained in H_2, we would choose $h \in H_1$, $h \notin H_2$, and conclude that hH_2 would act without fixed-points on H_2L_2/H_2 and in particular would act without fixed-points on H_2L_1/H_2, all subgroups of a cyclic group being characteristic. However, since $h \in H_1$, we see that $[h, L_1] \leqq H_1$, so that $[h, L_1]$ is a p-group. Hence $[h, L_1]H_2/H_2$ is a p-subgroup of L_1H_2/H_2, and so equals 1, which violates the fact that hH_2 is supposed to act without fixed-points on L_1H_2/H_2. Hence, $H_1 \leqq H_2$.

Consider next $P \cap H_2$. We must have the equality $P \cap H_2 = H_1$, by the maximal nature of H_1, since H_2 is contained in at least two distinct Sylow p-subgroups of G, and since the last paragraph showed that $P \cap H_2 \geqq H_1$.

Now we have the strict containments:

$$H_1 < P_1 < P^*,$$

where $P^* \leqq P$, and $P^* < N_2$. Since $P_1 = N_G(H_1) \cap P$ as we saw earlier, it follows that P^* does not normalize H_1. However, since $P^* < N_2$, P^* does normalize H_2. P^* trivially normalizes P, since $P^* \leqq P$. Hence P^* normalizes $P \cap H_2$, which we have just seen is equal to H_1. This contradiction forces $P_1 = P$.

Since $V_G(W; P_1) = V_G(W; H_1)$, and since $P_1 = P$, we find $V_G(W; P) = V_G(W; H_1)$. Since $V_G(W; H_1) \lhd N_1$, we find $N_1 \leqq N_G(V)$. We are now close to the desired contradiction. We have assumed that $H_1 \not\leqq H_0$, and we have found that $H_1 \leqq N_G(H_1) = N_1 \leqq N_G(V)$. It is straightforward to check that if a p-subgroup T of $N_G(V)$ is not contained in H_0, then $N_{N_G(V)}(T)$ is a p-group. Since $N_1 \leqq N_G(V)$, it follows that $N_G(H_1) = N_{N_G(V)}(H_1)$, so that N_1 must be a p-group. This contradiction forces us to accept the conclusion that $H_1 \leqq H_0$.

We are now in a position to apply GRÜN's Theorem. [2, p. 214] Since $P \cap (P^x)' \leqq P \cap P^x \leqq H_0$ for all $P^x \neq P$ and since $N_G(P) = P$, we conclude that G has a normal subgroup of index p, against our assumption that G is a non-solvable simple group. This last contradiction forces us to accept Theorem 1.

LEMMA 1.14. *If H is a maximal nilpotent subgroup of G, then H is a Hall subgroup, $H \cap H^x = 1$ or H for all $x \in G$, $N_G(H) \neq H$ and elements in $N_G(H) - H$ induce fixed-point-free automorphisms of H.*

PROOF. That H is Hall follows from lemma 1.3, and the fact that H is a maximal nilpotent subgroup of G.

If $H \cap H^x \neq 1$, and H is a Sylow p-subgroup of G, Theorem 1 says $H = H^x$. Otherwise, $H \cap H^x \neq 1$ implies $H = H^x$ by lemma 1.3 and the fact that H is a maximal nilpotent subgroup of G.

The last assertion follows from lemma 1.3 and the fact that H is a maximal nilpotent subgroup of G.

By FROBENIUS' theorem [2, p. 292], the simplicity of G, and lemma 1.14, $N_G(H) \neq H$.

LEMMA 1.15. *Two distinct maximal nilpotent subgroups H_1 and H_2 of G intersect in the identity element only, and if H_1 and H_2 are not conjugate then $((H_1), (H_2)) = 1$.*

PROOF. Straightforward, and so omitted.

Let $H_1, \ldots, H_r$ be a set of representatives for the conjugate classes of maximal nilpotent subgroups of G. Set

$$(G) = g,$$

$$(H_i) = h_i, \qquad (N_i) = h_i n_i, \tag{1.9}$$

$$i = 1, 2, \ldots, r.$$

LEMMA 1.16.

$$g = 1 + \sum_{i=1}^{r} \frac{h_i - 1}{h_i n_i} \cdot g. \tag{1.10}$$

PROOF. (1.10) is the "counting" equation. Each H_i^x contains $h_i - 1$ non-identity elements. (1.10) now follows from (1.9), lemma 1.15, and the fact that each element of G is contained in the (nilpotent) group it generates, and hence is contained in some H_i^x.

II. The Character-Theoretic Lemmas

Although much of this section is taken directly from SUZUKI [6], for the sake of completeness and clarity, the necessary lemmas will be proved in detail.

The character theory used here is with respect to the complex numbers. By a character of the group X is meant the trace function of any homomorphism of X into matrices with complex numbers as entries, and by a generalized character is meant a linear combination of characters with rational integer coefficients. The character ring of X, denoted by $\chi(X)$, is the set of all generalized characters of X, and we denote by $\chi_0(X)$ the ideal of all generalized characters which vanish at the identity element of X.

If Y is a subgroup of X, we denote by * the induced map from $\chi(Y)$ to $\chi(X)$, so that if $\varphi \in \chi(Y)$,

$$\varphi^*(x) = \frac{1}{[Y:1]} \sum_{g \in X} \varphi(x^g),$$

with the convention that $\varphi(z) = 0$ if $z \notin Y$.

If $Y < Z < X$, Y and Z being subgroups of X, we will use $\sim$ to indicate the induced map from $\chi(Y)$ to $\chi(Z)$, reserving * for the map from $\chi(Y)$ to $\chi(X)$ (or from $\chi(Z)$ to $\chi(X)$). It is well-known and easy to verify that if $\varphi \in \chi(Y)$, then $(\tilde{\varphi})^* = \varphi^*$. If one keeps in mind the agreement that a * always maps characters into $\chi(X)$, X being the "big" group, then no confusion arises.

If $\varphi, \psi \in \chi(X)$, then

$$(\varphi, \psi)_X = \frac{1}{[X:1]} \sum_{x \in X} \varphi(x) \cdot \overline{\psi(x)}$$

defines an inner product on $\chi(X)$. We put $||\varphi||_X = (\varphi, \varphi)_X$ and observe that $||\varphi||_X^{\frac{1}{2}}$ makes $\chi(X)$ into a metric space.

The major strength of the character theory for the problem at hand lies in the fact that if G is the group of the first section, H is a maximal nilpotent subgroup of G and $N = N_G(H)$, then there are some exploitable connections involving $\chi(H)$, $\chi(N)$, and $\chi(G)$. First, if φ is a non-principal irreducible character of H, then $\tilde{\varphi}$ is an irreducible character of N. Second, and perhaps most important from the point of view of computation, if $\tilde{\chi}_0(H)$ is the image in $\chi_0(N)$ of $\chi_0(H)$ under the map $\sim$, then the map $*$ induces an isometry between $\tilde{\chi}_0(H)$ and its image in $\chi_0(G)$. It is this fact which enables us to "keep track" of the irreducible characters of G which are involved in suitable ϱ^*, ϱ being an element of $\chi_0(H)$. We now proceed to formalize these facts, making as yet no specific reference to our group G.

The basic hypothesis of the following lemmas include:

1. A finite group S of odd order.
2. A subgroup M of S, satisfying:
   a) M is nilpotent.
   b) $M \cap M^s = 1$ or M, for all $s \in S$.
   c) $M < N_S(M) = N < S$.
   d) If $m \in M$, $m \neq 1$, then $C_S(m) \leqq M$.

We denote by Ω the hypotheses just listed.

LEMMA 2.1. *Given Ω, N/M induces automorphisms of $\chi(M)$ which have no fixed points on the non-principal irreducible characters of M.*

PROOF. Let φ be a non-principal irreducible character of a representation ϱ of M left fixed by some non-identity element $\bar{x} \in N/M$, that is, suppose $\varphi(m^x) = \varphi(m)$ for each $m \in M$. Note that $\varphi(m^x)$ does not depend on the coset representative x of $\bar{x}$, since φ is a class function. Then x normalizes the kernel K of ϱ, since K is characterized as the set of all $m \in M$ such that $\varphi(m) = \varphi(1)$. Since x is not in M, 2. d) implies that x induces a fixed-point-free automorphism of M, and hence by lemma 1.1, also on M/K, and also on $Z(M/K)$, which is cyclic of order t, say, with cyclic generator z. But then $\varphi(z) = \zeta \cdot \varphi(1)$, ζ being some primitive t-th root of unity. Since x normalizes $Z(M/K)$ and is fixed-point-free there, $z^x = z^n$ with $n \not\equiv 1 \pmod{t}$. Hence $\varphi(z^x) = \varphi(z^n) = \zeta^n \varphi(1) \neq \varphi(z)$, a contradiction.

LEMMA 2.2. *The map $\sim$: $\chi(M) \to \chi(N)$ sends non-principal irreducible characters of M into irreducible characters of N. The map $*$: $\chi(N) \to \chi(S)$ is an isometry from $\tilde{\chi}_0(M)$ into $\chi_0(S)$.*

PROOF. Let φ be a non-principal irreducible character of M. By definition of $\tilde{\varphi}$,

$$(2.1) \qquad \begin{cases} \tilde{\varphi}(h) = 0 & \text{if } h \notin M, \\ \tilde{\varphi}(m) = \frac{1}{[M:1]} \sum_{x \in N} \varphi(m^x) = \sum_{s \in N/M} \varphi(m^s), & m \in M. \end{cases}$$

Since $\tilde{\varphi}$ vanishes outside M, we see that

$$||\tilde{\varphi}||_N = \frac{1}{[N:M]} ||\tilde{\varphi}|M||_M.$$

By (2.1) and lemma 2.1, $\tilde{\varphi}|M$ is a sum of $[N:M]$ distinct irreducible characters of M, so that

$$||\tilde{\varphi}|M||_M = [N:M],$$

which proves the first assertion of the lemma.

Let α be a generalized character of M vanishing at 1. Then

$$||\tilde{\alpha}||_N = \frac{1}{[N:1]} \sum_{x \in N} |\tilde{\alpha}(x)|^2,$$

while

$$||\tilde{\alpha}^*||_S = ||\alpha^*||_S = \frac{1}{[S:1]} \sum_{y \in S} |\alpha^*(y)|^2$$

$$= \frac{1}{[N:1]} \sum_{m \in M} |\tilde{\alpha}(m)|^2 = ||\tilde{\alpha}||_N,$$

by Ω. This proves the second assertion of the lemma.

We say that two characters φ and φ_1 of M are equivalent if $\tilde{\varphi} = \tilde{\varphi}_1$, otherwise inequivalent. In a group of odd order, if φ is a non-principal irreducible character, then $\varphi \neq \bar{\varphi}$, its complex conjugate [1, p. 294], so the total number of non-principal irreducible characters of any degree is even.

Let d be the degree of some irreducible character of M, and suppose there are $w \cdot [N:M]$ such non-principal characters so that w is even. Let $\varphi_1, \ldots, \varphi_w$ be a set of representatives for the equivalence classes of non-principal irreducible characters of M of degree d, so that $\tilde{\varphi}_1, \ldots, \tilde{\varphi}_w$ are w distinct irreducible characters of N.

Consider $\tilde{\varphi}_1 - \tilde{\varphi}_2$. Since $\tilde{\varphi}_1$ and $\tilde{\varphi}_2$ are both irreducible characters of N,

$$||\tilde{\varphi}_1 - \tilde{\varphi}_2||_N = 2.$$

Since $\varphi_1 - \varphi_2 \in \chi_0(M)$,

$$||\varphi_1^* - \varphi_2^*||_S = 2,$$

by lemma 2.2, so that

$$\varphi_1^* - \varphi_2^* = \varepsilon \Theta + \eta \Theta', \qquad \varepsilon^2 = \eta^2 = 1,$$

Θ and Θ' being distinct irreducible characters of S. Since $\varphi_1^* - \varphi_2^* \in \chi_0(S)$, $\eta = -\varepsilon$, so that

$$\varphi_1^* - \varphi_2^* = \varepsilon(\Theta - \Theta').$$

If $w = 2$, we associate φ_1 with Θ and φ_2 with Θ', the association being determined once we have decided on whether we want $\varepsilon = +1$ or $\varepsilon = -1$.

If $w > 2$, we also have

$$\varphi_1^* - \varphi_3^* = \varepsilon'(\Theta_1 - \Theta_1'),$$

and by interchanging Θ_1 and Θ_1' if necessary, we can assume that $\varepsilon = \varepsilon'$. We now have the two equations

$$\varphi_1^* - \varphi_2^* = \varepsilon(\Theta - \Theta')$$
$$\varphi_1^* - \varphi_3^* = \varepsilon(\Theta_1 - \Theta_1'),$$

and since the difference $\varphi_1^* - \varphi_2^* - (\varphi_1^* - \varphi_3^*) = \varphi_3^* - \varphi_2^*$ has norm 2, so does $\varepsilon(\Theta - \Theta' - (\Theta_1 - \Theta_1'))$. By interchanging, Θ and Θ', Θ_1 and Θ_1', and using $-\varepsilon$ if necessary, we can suppose that $\Theta = \Theta_1$. Put $\Theta' = \Theta_2$ and $\Theta_1' = \Theta_3$, so that the equations become

$$\varphi_1^* - \varphi_2^* = \varepsilon(\Theta_1 - \Theta_2),$$
$$\varphi_1^* - \varphi_3^* = \varepsilon(\Theta_1 - \Theta_3).$$

Since φ_2 and φ_3 are inequivalent under the action of N/M, $\Theta_2 \neq \Theta_3$. It follows easily now that if $w \geqq 4$, then

$$\varphi_i^* - \varphi_j^* = \varepsilon(\Theta_i - \Theta_j), \quad i, j = 1, 2, \ldots, w \tag{2.2}$$

for suitable irreducible characters Θ_j of S. We associate $\tilde{\varphi}_i$ with Θ_i and also we associate φ_i with Θ_i, establishing in this fashion a $1-1$ correspondence between the equivalence classes of non-principal irreducible characters of M and certain irreducible characters of S.

Let $z_1 = 1, z_2, z_3, \ldots, z_t$ be the distinct degrees of irreducible characters of M. Let w_i be the number of equivalence classes of non-principal irreducible characters of M of degree z_i, so that $w_i[N:M]$ is the total number of non-principal irreducible characters of M of degree z_i. We note that

$$w_1 = \frac{[M:M'] - 1}{[N:M]}. \tag{2.3}$$

Let $\varphi_{i1}, \ldots, \varphi_{iw_i}$ correspond to $\Theta_{i1}, \ldots, \Theta_{iw_i}$ in the fashion described above, $\varphi_{i1}, \ldots, \varphi_{iw_i}$ being a set of representatives for the equivalence classes of non-principal irreducible characters of M of degree z_i, $\Theta_{i1}, \ldots, \Theta_{iw_i}$ being irreducible characters of S. Also, set

$$\Xi_i = \sum_{j=1}^{w_i} \Theta_{ij}$$

and

$$\Gamma_i = z_i 1_M^* - \varphi_{i1}^*. \tag{2.4}$$

We denote by 1_M the principal character of M, and by ϱ_0 the principal character of S.

LEMMA 2.3. *1_M^* is equal to ϱ_0 plus a linear combination of the Ξ_i's plus a linear combination of characters which involve neither ϱ_0 nor any Θ_{ij}.*

PROOF. By orthogonality of the irreducible characters of G, if ϱ is an irreducible character of S, then

$$(1_M^*, \varrho)_S$$

is the multiplicity of ϱ in l_M^*. By Frobenius reciprocity [2, p. 284]

$$(1_M^*, \varrho)_S = (1_M, \varrho | M)_M. \tag{2.5}$$

Since $\varrho_0 | M = 1_M$, (2.5) shows that the multiplicity of ϱ_0 in 1_M^* is 1. The rest of the lemma is the statement that

$$(1_M^*, \Theta_{ij}) = (1_M^*, \Theta_{ik}), \quad 1 \leqq i \leqq t, \quad 1 \leqq j, k \leqq w_i. \tag{2.6}$$

Now (2.6) follows from (2.2) and Frobenius reciprocity.

LEMMA 2.4. *φ_{ij}^* equals $\pm\Theta_{ij}$ plus a linear combination of the Ξ's plus a linear combination of characters which involve neither ϱ_0 nor any Θ_{rs}, $1 \leqq r \leqq t$, $1 \leqq s \leqq w_r$.*

PROOF.

$$\begin{aligned}(\varphi_{ij}^*, \Theta_{kr} - \Theta_{ks})_S &= (\varphi_{ij}^*, \pm(\varphi_{kr}^* - \varphi_{ks}^*))_S \\ &= (\tilde{\varphi}_{ij}, \pm(\tilde{\varphi}_{kr} - \tilde{\varphi}_{ks}))_N \\ &= \pm\delta_{ik}(\delta_{jr} - \delta_{js}),\end{aligned}$$

by (2.2) and Frobenius reciprocity. Also,

$$(\varphi_{ij}^*, \varrho_0)_S = (\varphi_{ij}, 1_M)_M = 0,$$

and the lemma follows.

The two previous lemmas yield immediately that

$$\Gamma_i = z_i\varrho_0 + \varepsilon_i\Theta_{il} + \sum_{j=1}^{t} a_{ij}\Xi_j + \Delta_i, \tag{2.7}$$

with

$$(\Delta_i, \Theta_{ks})_S = (\Delta_i, \varrho_0)_S = 0, \quad \begin{aligned}&1 \leqq k \leqq t,\\ &1 \leqq s \leqq w_k,\\ &1 \leqq i \leqq t.\end{aligned} \tag{2.8}$$

Since each of the groups $H_1, \ldots, H_r$ of Section I satisfies Ω, we can apply the previous lemmas. If H_i has $1+s_i$ conjugate classes, we determine

$$a = \sum_{i=1}^{r} \frac{s_i}{[N_i : H_i]}$$

distinct irreducible non-principal characters of G, (distinctness is easily verified) each one being associated with one of the H_i's. Since a is the number of non-identity conjugate classes of G, it follows that each non-principal irreducible character of G is exceptional with respect to a unique one of $H_1, \ldots, H_r$. We adjoin an extra subscript throughout (2.4) and (2.7), so that

$$\begin{cases} \Gamma_{ik} = z_{ik}\cdot\varrho_0 + \varepsilon_{ik}\Theta_{i1k} + \sum_{j=1}^{t_k} a_{ijk}\Xi_{jk} + \Delta_{ik}, \\ \Gamma_{ik} = z_{ik}\,1_{H_k}^* - \varphi_{i1k}^*, \end{cases} \tag{2.9}$$

the subscript k indicating the group H_k.

LEMMA 2.5. *Δ_{jk} is a linear combination of the $\Xi_{\sigma\tau}$, with $\tau \neq k$.*

PROOF. By lemmas 2.3 and 2.4 and (2.8), we know that Δ_{jk} does not involve ϱ_0 or any $\Theta_{\sigma\varrho k}$. The lemma now follows from the fact that if $\tau \neq k$, then

$$\begin{aligned}(\Delta_{jk}, \Theta_{\sigma\lambda\tau} - \Theta_{\sigma\mu\tau})_G &= (\Gamma_{jk}, \Theta_{\sigma\lambda\tau} - \Theta_{\sigma\mu\tau})_G \\ &= \pm(z_{jk}\,1_{H_k}^* - \varphi_{j1k}^*, \varphi_{\sigma\lambda\tau}^* - \varphi_{\sigma\mu\tau}^*)_G \\ &= 0.\end{aligned}$$

since in the last inner product, the first factor vanishes outside the conjugate class of H_k, while the second vanishes at 1 and outside the conjugate class of H_τ.

DEFINITION. $\mathscr{I}(\Delta_{jk})$ is the set of all H_τ, $\tau \neq k$, such that $\Xi_{\sigma\tau}$ is involved in Δ_{jk} for at least one value of σ.

LEMMA 2.6. *$\Theta_{jik}=\Theta$ assumes rational integer values outside the conjugate class of H_k, and assumes non-zero rational integer values on H_λ, provided $\lambda \neq k$, and $H_\lambda \notin \mathscr{I}(\Delta_{jk})$.*

PROOF. Consider for $\lambda \neq k$,

$$\Theta | H_\lambda = \sum_\chi a_\chi \chi,$$

χ ranging over the irreducible characters of H_λ. By orthogonality of the irreducible characters, and by Frobenius reciprocity,

$$\begin{aligned} a_{\chi_1} - a_{\chi_2} &= (\Theta | H_\lambda, \chi_1)_{H_\lambda} - (\Theta | H_\lambda, \chi_2)_{H_\lambda} \\ &= (\Theta, \chi_1^* - \chi_2^*)_G. \end{aligned}$$

If χ_1 and χ_2 are two non-principal irreducible characters of H_λ of the same degree, then by lemma 2.2 applied to H_λ, $\chi_1^* - \chi_2^*$ is the difference of two irreducible characters of G, neither of which is Θ. Thus,

$$a_{\chi_1} - a_{\chi_2} = (\Theta, \chi_1^* - \chi_2^*)_G = 0.$$

Since the sum of all irreducible characters of a given degree assumes rational integer values, so does $\Theta | H_\lambda$.

If furthermore, $H_\lambda \notin \mathscr{I}(\Delta_{jk})$, and $h \in H_\lambda$, then by the result just proved, if $\Theta_{\sigma\varrho\tau}$ is involved in Δ_{jk}, $\Theta_{\sigma\varrho\tau}(h)$ is a rational integer. It follows that

$$\Delta_{jk}(h) \equiv 0 \,(2),$$

$$\sum_{l=1}^{t_k} a_{jlk} \Xi_{lk}(h) \equiv 0 \,(2).$$

If $\Theta_{j1k}(h)=0$, then (2.9) would yield

$$\Gamma_{jk}(h) = 0 \equiv z_{jk} \pmod 2. \tag{2.10}$$

Since z_{jk} is odd, (2.10) cannot hold. Since Θ_{j1k} and Θ_{jik} agree outside the conjugate class of H_k, by lemmas 2.2 and (2.2) the lemma follows.

LEMMA 2.7. *$\mathscr{I}(\Delta_{1i})$ has no more than*

$$u_i = \frac{[N_i : H_i] + 1 - \left\| \varrho_0 + \varepsilon_{1i}\Theta_{11i} + \sum_{j=1}^{t_i} a_{1ji}\Xi_{ji} \right\|_G}{2} \tag{2.11}$$

elements.

PROOF.

$$||\tilde{1}_{H_i} - \tilde{\varphi}_{11i}||_{N_i} = ||\Gamma_{1i}||_G = 1 + [N_i : H_i]$$

$$= ||\varrho_0 + \varepsilon_{1i}\Theta_{11i} + \sum_{j=1}^{t_i} a_{1ji}\Xi_{ji}||_G + ||\Delta_{1i}||_G,$$

by (2.9), lemma 2.2, and the fact that $||\tilde{1}_{H_i}||_{N_i} = [N_i : H_i]$.

By definition of $\mathscr{I}(\Delta_{1i})$, if $H_\tau \in \mathscr{I}(\Delta_{1i})$, then some $\Xi_{\sigma\tau}$ makes a contribution of at least two to $||\Delta_{1i}||_G$. The lemma follows.

We assume now that our notation is chosen so that

$$[N_1 : H_1] \leqq [N_2 : H_2] \leqq \cdots \leqq [N_r : H_r]. \tag{2.12}$$

We recall the notation of (1.9) and (2.3), and we set

$$\Xi = \Xi_{11}.$$

If $[N_1 : H_1] = [N_2 : H_2]$, we order H_1 and H_2 so that $[H_1 : H_1'] > [H_2 : H_2']$. We remark that if $[N_1 : H_1] = [N_2 : H_2]$, then

$$\frac{[H_1 : H_1'] - 1}{[N_1 : H_1]} > \frac{[H_2 : H_2'] - 1}{[N_2 : H_2]} \geqq 2,$$

so that

$$w = w_{11} = \frac{[H_1 : H_1'] - 1}{[N_1 : H_1]} \geqq 4. \tag{2.13}$$

LEMMA 2.8.

$$\sum_{\substack{H_\tau \notin \mathscr{I}(\Delta_{11}) \\ \tau \neq 1}} \frac{h_\tau - 1}{h_\tau n_\tau} \leqq \frac{1}{w}.$$

PROOF.

$$g \cdot ||\Xi||_G = g\, w = \sum_{x \in G} |\Xi(x)|^2 \geqq w^2 \sum_{\substack{H_\tau \notin \mathscr{I}(\Delta_{11}) \\ \tau \neq 1}} \frac{h_\tau - 1}{h_\tau n_\tau} \cdot g,$$

by (2.2), lemma 2.6, and the fact that the conjugate classes of the H_λ's partition G. The lemma follows.

LEMMA 2.9.

$$\sum_{H_\lambda \in \mathscr{I}(\Delta_{11})} \frac{h_\lambda - 1}{h_\lambda n_\lambda} \leqq \frac{u_1}{n_2}.$$

PROOF. By lemma 2.7, there are at most u_1 elements in $\mathscr{I}(\Delta_{11})$. By (2.12), each such element makes a contribution of at most $1/n_2$ to the above sum. The lemma follows.

Combining lemmas 2.8 and 2.9, we conclude

$$\sum_{i=1}^{r} \frac{h_i - 1}{h_i n_i} \leqq \frac{h_1 - 1}{h_1 n_1} + \frac{1}{w} + \frac{u_1}{n_2}.$$

By the counting equation (1.10), we find

$$1 = \frac{1}{g} + \sum_{i=1}^{r} \frac{h_i - 1}{h_i n_i} \leqq \frac{1}{g} + \frac{h_1 - 1}{h_1 n_1} + \frac{1}{w} + \frac{u_1}{n_2}.$$

Since

$$u_1 \leqq \frac{n_1 - 1}{2},$$

by (2.11), we conclude

$$1 \leqq \frac{1}{g} + \frac{h_1 - 1}{h_1 n_1} + \frac{1}{w} + \frac{n_1 - 1}{2n_2}. \tag{2.14}$$

Suppose $w > 2$, so that $w \geqq 4$, since w is even. Since $n_2 \geqq n_1$, we conclude from (2.14), that

$$\frac{1}{4} \leqq \frac{1}{g} + \frac{h_1 - 1}{h_1 n_1} - \frac{1}{2n_1} = \frac{1}{g} - \frac{1}{h_1 n_1} + \frac{1}{2n_1}.$$

Since $n_1 \geqq 3$, we have

$$\frac{1}{12} \leqq \frac{1}{g} - \frac{1}{h_1 n_1} \leqq \frac{1}{g},$$

or

$$g \leqq 12,$$

which is not the case. Hence $w = 2$. It follows from (2.13) and the remark preceding (2.13), that $n_2 > n_1$. Since n_1 and n_2 are odd, we find that $n_2 \geqq n_1 + 2$. Using (2.14), with $w = 2$, we find

$$\frac{1}{2} \leqq \frac{1}{g} + \frac{h_1 - 1}{h_1 n_1} + \frac{n_1 - 1}{2(n_1 + 2)},$$

or

$$0 \leqq \frac{1}{g} + \frac{h_1 - 1}{h_1 n_1} - \frac{3}{2(n_1 + 2)} = \frac{1}{g} - \frac{1}{h_1 n_1} + \left(\frac{1}{n_1} - \frac{3}{2(n_1 + 2)}\right). \tag{2.15}$$

If $n_1 \geqq 5$, it follows that

$$\frac{1}{n_1} - \frac{3}{2(n_1 + 2)} \leqq 0, \tag{2.16}$$

so that (2.15) and (2.16) imply

$$0 \leqq \frac{1}{g} - \frac{1}{h_1 n_1},$$

$$g \leqq h_1 n_1,$$

which is not the case, since $h_1 n_1 = [N_1 : 1]$, and N_1 is a proper subgroup of G.

There remains that possibility that $n_1 = 3$. Since $w = 2$, we conclude that $[H_1 : H_1'] = 1 + n_1 w = 7$. It follows that $H_1' = \{1\}$, and $h_1 = 7$. In this case, (2.15) gives

$$0 \leqq \frac{1}{g} - \frac{1}{21} + \frac{1}{3} - \frac{3}{10} = \frac{1}{g} - \frac{1}{70},$$

or

$$g \leqq 70,$$

which is not the case. This completes the proof of Theorem A.

REMARK. This proof differs from the corresponding proof of SUZUKI in that nowhere in this proof do we estimate the value of an exceptional character

on the subgroup with respect to which it is exceptional. In SUZUKI's proof, attention is focussed on a maximal abelian subgroup of minimal order. Here, attention is focussed on a maximal nilpotent subgroup such that its normalizer index is minimal. By so doing, we are able to avoid the possibility that H_1 is heavily non-abelian, and so a potentially nasty group H_1 is not really looked at very closely.

References

[1] BURNSIDE, W.: Theory of Groups of Finite Order, 2nd edition. Cambridge 1911. — [2] HALL, M.: The Theory of Groups. The Macmillan Co. New York: 1959. — [3] HALL, P., and G. HIGMAN: On the p-length of p-soluble groups and reduction theorems for Burnside's problem. Proc. London math. Soc. (3) **6**, 1—42 (1956). — [4] HALL, P.: A note on soluble groups. J. London math. Soc. **3**, 98—105 (1928). — [5] HIGMAN, G.: Finite groups in which every element has prime power order. J. London math. Soc. **32**, 335—342 (1957). — [6] SUZUKI, M.: The nonexistence of a certain type of simple groups of odd order. Proc. Amer. math. Soc. **8**, 686—695 (1957). — [7] WIELANDT, H.: Zum Satz von SYLOW. Math. Z. **60**, 407—408 (1954).

Cornell University, Ithaca, N.Y. (U.S.A.)

California Institute of Technology, Pasadena, Cal. (U.S.A.)

Institute for Defense Analyses, Princeton, N. J. (U.S.A.)

(Eingegangen am 27. November 1959)

Fröhlich, A.
Math. Zeitschr. 74, 18–28 (1960)

Discriminants of algebraic number fields

By
Albrecht Fröhlich

The definition of a discriminant in the theory of finite algebraic number fields has always suffered from a dichotomy. The "relative" discriminant of an extension Λ/K is an ideal (or divisor); if K happens to be the rational field however a numerical "absolute" discriminant is defined. In the present note a new concept of a discriminant $\mathfrak{d}(\Lambda/\mathsf{K})$ will be introduced which covers both classical notions [1]).

One can in a purely formal manner and without affecting in any way the theory of the absolute discriminant reword its definition so as to consider it as a class of rational idèles modulo the squares of the unit-idèles [cf. (2.4)]; as will be shown this definition generalises in a natural manner to an arbitrary finite number field K as base field.

The foremost problem arising in this context is to obtain in terms of the new discriminant $\mathfrak{d}(\Lambda/\mathsf{K})$ a criterion for the existence of a relative integral basis for Λ/K, i.e. of a free module basis of the algebraic integers in Λ over those in K. It will be shown in fact (cf. 2.5) that such a basis exists if, and only if, $\mathfrak{d}(\Lambda/\mathsf{K})$ is *principal*, i.e. is represented by a number in K. This condition can then be utilised to determine, by means of simple arithmetic criteria, families of fields Λ for which relative integral bases over K exist (cf. 3.2, 4.3).

Using the new concept the basic properties of absolute discriminants can now be seen to extend quite generally to arbitrary base fields K. Thus the theorem of Stickelberger-Schur on congruence relations of $\mathfrak{d}(\Lambda/\mathsf{K})$ mod 4 is true in full generality (cf. 2.6). The signature of a discriminant is always defined and has the expected interpretation. Of particular interest are, as in the rational case, the quadratic discriminants. We shall give a complete determination of these (cf. 3.1). It will be seen in particular that distinct quadratic fields have distinct discriminants (cf. 3.4). The corresponding results for the classical relative discriminant are either not true, or cannot even be sensibly formulated.

The relative discrimant of Λ/K in the hitherto accepted sense is simply the ideal defined by $\mathfrak{d}(\Lambda/\mathsf{K})$. On the basis of our theory Hecke's theorem on the absolute ideal class of the discriminant will follow quite easily (cf. 2.3), and an analogous criterion for the ideal class in the narrow sense will also

[1]) Our definitions and results will be formulated in terms of number fields only. The possible generalisation to quotient fields Λ and K of appropriate Dedekind domains is obvious. It is only necessary to introduce the analogue to the group $J_{\mathsf{K}}/U_{\mathsf{K}}^2$ (c.f. § 2). At each step the required conditions on Λ and K — such as separability of Λ/K — are clear from the text.

be established (cf. 4.6). At the same time we shall prove a conjecture of HERBRAND's (cf. 4.7).

As a final illustration we shall derive, in analogy to the rational case, the classification of cubic fields over K into cyclic ones and non-normal ones by means of their discriminant.

In a subsequent paper [3] the concepts developed here will be used to determine arithmetically the structure of the ideals in a finite extension Λ qua modules over the integers in the base field K. Other problems which may be of interest in this context are the generalisation of the Kronecker-symbol and the application of the ideas of the present paper to quadratic forms.

§ 1. Local Discriminants

NOTATION AND CONVENTIONS. Throughout K is a finite algebraic number field and $\mathfrak{o}$ the ring of (algebraic) integers in K. If R is an integral domain, $R^\times$ is the multiplicative semigroup of non zero elements; if moreover R is a principal ideal ring $(M:R)$ stands for the rank of the free R-module M.

Let $\mathfrak{p}$ be a prime divisor in K and let $\mathsf{K}_\mathfrak{p}$ be the corresponding completion of K. If $\mathfrak{p}$ is finite $\mathfrak{o}_\mathfrak{p}$ is the ring of $\mathfrak{p}$-adic integers in $\mathsf{K}_\mathfrak{p}$ and $U_\mathfrak{p}$ the group of units; if $\mathfrak{p}$ is infinite we put $\mathfrak{o}_\mathfrak{p}=\mathsf{K}_\mathfrak{p}$, $U_\mathfrak{p}=\mathsf{K}_\mathfrak{p}^\times$. We shall consider finite dimensional commutative $\mathsf{K}_\mathfrak{p}$-algebras without radical, briefly called $\mathsf{K}_\mathfrak{p}$-algebras. Such an algebra $\Lambda_\mathfrak{p}$ is the direct sum of fields $\Lambda_\mathfrak{p}^{(i)}$,

$$\Lambda_\mathfrak{p}=\sum\Lambda_\mathfrak{p}^{(i)}. \tag{1.1}$$

$\Lambda_\mathfrak{p}$ will contain a unique maximal order $\mathfrak{O}_\mathfrak{p}$ and $(\Lambda_\mathfrak{p}:\mathsf{K}_\mathfrak{p})=(\mathfrak{O}_\mathfrak{p}:\mathfrak{o}_\mathfrak{p})$. $\mathfrak{O}_\mathfrak{p}$ is the direct sum of the corresponding maximal orders $\mathfrak{O}_\mathfrak{p}^{(i)}$:

$$\mathfrak{O}_\mathfrak{p}=\sum\mathfrak{O}_\mathfrak{p}^{(i)}. \tag{1.2}$$

The discriminant of every $\mathfrak{o}_\mathfrak{p}$-basis of $\mathfrak{O}_\mathfrak{p}$ is an element of $\mathfrak{o}_\mathfrak{p}^\times$ and is uniquely determined modulo $U_\mathfrak{p}^2$ by $\Lambda_\mathfrak{p}$. We denote its class in $\mathsf{K}_\mathfrak{p}^\times/U_\mathfrak{p}^2$ by $\mathfrak{d}(\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p})$; this is the discriminant of $\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$. From (1.2) we have immediately

$$\mathfrak{d}(\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p})=\prod_i\mathfrak{d}(\Lambda_\mathfrak{p}^{(i)}/\mathsf{K}_\mathfrak{p}). \tag{1.3}$$

If in particular $\Lambda_\mathfrak{p}$ is a field then the norm mapping $N_{\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}$ takes the group $\overline{U}_\mathfrak{p}$ of units in $\Lambda_\mathfrak{p}$ into $U_\mathfrak{p}$ and thus gives rise to a homomorphism $\Lambda_\mathfrak{p}^\times/\overline{U}_\mathfrak{p}^2\to\mathsf{K}_\mathfrak{p}^\times/U_\mathfrak{p}^2$ again to be denoted by $N_{\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}}$. One obtains then for a $\Lambda_\mathfrak{p}$-algebra $\Omega_\mathfrak{p}$ the formula

$$\mathfrak{d}(\Omega_\mathfrak{p}/\mathsf{K}_\mathfrak{p})=\mathfrak{d}(\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p})^{(\Omega_\mathfrak{p}:\Lambda_\mathfrak{p})}\cdot N_{\Lambda_\mathfrak{p},\mathsf{K}_\mathfrak{p}}\mathfrak{d}(\Omega_\mathfrak{p}/\Lambda_\mathfrak{p}). \tag{1.4}$$

In establishing (1.4) we may assume $\Omega_\mathfrak{p}$ to be actually an extension field of $\mathsf{K}_\mathfrak{p}$ contained in some normal extension $\overline{\mathsf{K}}_\mathfrak{p}$ of $\mathsf{K}_\mathfrak{p}$. Indicating row and column indices in the obvious manner we consider matrices

$$A=(a_i^\gamma)_{i,\gamma},\qquad B=(b_\tau^\sigma)_{\tau,\sigma},$$

where the a_i (the b_r) form an integral basis for Λ_p/K_p (for Ω_p/Λ_p); γ (and σ) runs through the complete set of monomorphisms $\Lambda_p \to \overline{\mathsf{K}}_p$ over K_p (and $\Omega_p \to \overline{\mathsf{K}}_p$ over Λ_p). Extend each γ to an automorphism of $\overline{\mathsf{K}}_p$ and write

$$C = (a_i^{\gamma}\, b_r^{\sigma\gamma})_{(i,r),(\sigma,\gamma)}.$$

Then

$$|A|^2\, U_p^2 = \mathfrak{d}(\Lambda_p/\mathsf{K}_p),$$
$$|B|^2\, \overline{U}_p^2 = \mathfrak{d}(\Omega_p/\Lambda_p),$$
$$|C|^2\, U_p^2 = \mathfrak{d}(\Omega_p/\mathsf{K}_p).$$

Define moreover matrices

$$A^{\times} = (a_i^{\gamma}\, \delta_{r,r'})_{(i,r),(r',\gamma)},$$
$$B^{\times} = (b_r^{\sigma\gamma}\, \delta_{\gamma,\gamma'})_{(r,\gamma),(\sigma,\gamma')}.$$

Then on the one hand $A^{\times} B^{\times} = C$ while on the other hand

$$|A^{\times}|^2 = |A|^{2(\Omega_p:\Lambda_p)}, \qquad |B^{\times}|^2 = N_{\Lambda_p/\mathsf{K}_p}|B|^2.$$

Comparison of the equations we have derived gives (1.4).

Let now Λ be a finite algebraic extension field of K. For[2]) every prime divisor $\mathfrak{p}$ in K,

$$\Lambda_p = \Lambda \otimes_{\mathsf{K}} \mathsf{K}_p \tag{1.5}$$

is a K_p-algebra and $(\Lambda_p:\mathsf{K}_p) = (\Lambda:\mathsf{K})$. Let $\mathfrak{Q}$ be the domain of integers in Λ. Then we have the natural identification for the maximal order in Λ_p

$$\mathfrak{Q}_p = \mathfrak{Q} \otimes_{\mathfrak{o}} \mathfrak{o}_p. \tag{1.6}$$

The discriminants $\mathfrak{d}(\Lambda_p/\mathsf{K}_p)$ will be called the *local discriminants* of Λ/K.

§ 2. The Global Discriminant

The idèle group (cf. [2]) in K will be denoted by J_{K} and the group of principal idèles by P_{K}; we may identify $P_{\mathsf{K}} = \mathsf{K}^{\times}$. U_{K} is the group of unit idèles, i.e. of idèles whose $\mathfrak{p}$-components lie in U_p everywhere. $J_{\mathsf{K}}/U_{\mathsf{K}}$ is then the ideal group.

Let again Λ be a finite algebraic extension of K. The classical discriminant of Λ/K is an ideal, i.e. is defined modulo U_{K}. To strengthen this definition we only have to note that $J_{\mathsf{K}}/U_{\mathsf{K}}^2$ can be identified with that subgroup in the cartesian product $\prod \mathsf{K}_p^{\times}/U_p^2$ whose elements have their $\mathfrak{p}$-components in U_p/U_p^2 almost everywhere. There exists thus a unique element $\mathfrak{d}(\Lambda/\mathsf{K})$ of $J_{\mathsf{K}}/U_{\mathsf{K}}^2$ such that for all $\mathfrak{p}$

$$[\mathfrak{d}(\Lambda/\mathsf{K})]_p = \mathfrak{d}(\Lambda_p/\mathsf{K}_p), \tag{2.1}$$

the right hand side lying in U_p/U_p^2, except when $\mathfrak{p}$ is ramified in Λ.

[2]) For the theory of the "local" algebras associated with the extension Λ/K see e.g. [4]. The following equation (1.6) follows from the "strong independence" of the valuations in Λ which correspond to the components $\Lambda_{\mathfrak{p}}^{(i)}$ (cf. [4], S. 280).

$\mathfrak{d}(\Lambda/\mathsf{K})$ is the *discriminant* of Λ/K; its local components are the local discriminants. An analogous rule applies to the classical discriminant, which will henceforth be denoted by $(\mathfrak{d}(\Lambda/\mathsf{K}))$. For all $\mathfrak{p}$, the $\mathfrak{p}$-component of this ideal is the ideal of $\mathfrak{d}(\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p})$. Therefore $(\mathfrak{d}(\Lambda/\mathsf{K}))$ is in fact the ideal derived from $\mathfrak{d}(\Lambda/\mathsf{K})$, i.e. its image under the mapping $J_\mathsf{K}/U_\mathsf{K}^2 \to J_\mathsf{K}/U_\mathsf{K}$.

The norm mapping $N_{\Lambda/\mathsf{K}}$ will induce a homomorphism $J_\Lambda/U_\Lambda^2 \to J_\mathsf{K}/U_\mathsf{K}^2$. From the properties of the norm-mappings involved and from (1.3), (1.4) we obtain the formula

$$\mathfrak{d}(\Omega/\mathsf{K}) = \mathfrak{d}(\Lambda/\mathsf{K})^{(\Omega:\Lambda)} \cdot N_{\Lambda/\mathsf{K}}\,\mathfrak{d}(\Omega/\Lambda), \tag{2.2}$$

for any finite algebraic extension Ω of Λ.

We shall in the sequel (cf. 2.1., 2.2., 2.6.) derive a number of restrictions on the possible classes of $J_\mathsf{K}/U_\mathsf{K}^2$ which can give discriminants. Trivially we have of course

2.1. $(\mathfrak{d}(\Lambda/\mathsf{K}))$ *is an integral ideal.*

In fact, as was pointed out in § 1, $\mathfrak{d}(\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p})$ will always lie in $\mathfrak{o}_\mathfrak{p}^\times/U_\mathfrak{p}^2$.

2.2. Theorem. $\mathfrak{d}(\Lambda/\mathsf{K})$ *lies in* $J_\mathsf{K}^2 P_\mathsf{K}/U_\mathsf{K}^2$.

Proof. Let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ be a basis of Λ/K with discriminant α. For every prime divisor $\mathfrak{p}$ the elements $\alpha_\mathfrak{p}^{(i)} = \alpha^{(i)} \otimes 1$ of $\Lambda_\mathfrak{p} = \Lambda \otimes_\mathsf{K} \mathsf{K}_\mathfrak{p}$ form a basis of $\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$ whose discriminant is $\alpha_\mathfrak{p}$. On the other hand if δ is a representative of $\mathfrak{d}(\Lambda/\mathsf{K})$ in J_K then $\delta_\mathfrak{p}$ is the discriminant of some basis of $\mathfrak{O}_\mathfrak{p}/\mathfrak{o}_\mathfrak{p}$; but this is also a basis of $\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}$. Therefore for all $\mathfrak{p}$, $\delta_\mathfrak{p}\alpha_\mathfrak{p}^{-1} \in \mathsf{K}_\mathfrak{p}^{\times 2}$, whence $\delta\alpha^{-1} \in J_\mathsf{K}^2$ as required.

The image of $\mathfrak{d}(\Lambda/\mathsf{K})$ under the mapping $J_\mathsf{K}/U_\mathsf{K}^2 \to J_\mathsf{K}/U_\mathsf{K} P_\mathsf{K}$ is the absolute ideal class of $(\mathfrak{d}(\Lambda/\mathsf{K}))$. From 2.2 we thus have

2.3. (Hecke [5], Theorem 177). *The absolute ideal class of* $(\mathfrak{d}(\Lambda/\mathsf{K}))$ *is a square.*

Let Y_K be the group of units in K; thus $Y_\mathsf{K} = U_\mathsf{K} \cap P_\mathsf{K}$. Moreover $J_\mathsf{K}^2 \cap P_\mathsf{K} = P_\mathsf{K}^2$, and so $U_\mathsf{K}^2 \cap P_\mathsf{K} = Y_\mathsf{K}^2$. We thus have a natural isomorphism

$$\varrho\colon \mathsf{K}^\times/Y_\mathsf{K}^2 \cong U_\mathsf{K}^2 P_\mathsf{K}/U_\mathsf{K}^2. \tag{2.3}$$

Assume now that the integral domain $\mathfrak{O}$ in Λ has a free $\mathfrak{o}$-basis (relative integral basis). The discriminant α of such a basis is an element of $\mathsf{K}^\times$, uniquely determined by $\mathfrak{O}$ modulo Y_K^2. We thus obtain a class $d(\Lambda/\mathsf{K})$ of $\mathsf{K}^\times/Y_\mathsf{K}^2$ called the *numerical discriminant* of Λ/K. By (1.6) $\alpha_\mathfrak{p}$ is (for all $\mathfrak{p}$) the discriminant of a basis of $\mathfrak{O}_\mathfrak{p}$ over $\mathfrak{o}_\mathfrak{p}$. Hence $\alpha U_\mathsf{K}^2 = \mathfrak{d}(\Lambda/\mathsf{K})$, and so we have

2.4. ϱ *induces a* $(1, 1)$*-mapping* $d(\Lambda/\mathsf{K}) \to \mathfrak{d}(\Lambda/\mathsf{K})$ *of the set of numerical discriminants into the set of discriminants.* $(\mathfrak{d}(\Lambda/\mathsf{K})$ *is the class* mod U_K^2 *determined by* $d(\Lambda/\mathsf{K})$.

If in particular $\mathfrak{o}$ is a principal ideal ring, so that numerical discriminants exist for all Λ we obtain a biunique correspondence

$$d(\Lambda/\mathsf{K}) \leftrightarrow \mathfrak{d}(\Lambda/\mathsf{K}). \tag{2.4}$$

Finally if in addition $Y_K^2 = 1$ then the numerical discriminants are actually elements of $K^\times$. This will in particular be the case for the rational field. (2.4) shows that the notion of a discriminant introduced here reduces essentially to that of an absolute discriminant, when K is the rational field.

We shall call an element of J_K/U_K^2 a *principal element* if it belongs to the subgroup $U_K^2 P_K/U_K^2$, i.e. if it is the image of a principal idèle under the mapping $J_K \to J_K/U_K^2$. A discriminant $\mathfrak{d}(\Lambda/K)$ is called a *principal discriminant* if it is a principal element, i.e. if it has a representative in $K^\times$; such a representative is then uniquely determined mod Y_K^2. The images under ϱ of numerical discriminants are principal; the question arises as to whether every principal discriminant is such an image. In other words, we have seen that if $\mathfrak{Q}$ has an integral basis over $\mathfrak{o}$, then $\mathfrak{d}(\Lambda/K)$ is principal; is the converse true as well? That this is in fact the case is the contents of the following theorem.

2.5. THEOREM. *The domain $\mathfrak{Q}$ of algebraic integers in Λ has a free module basis (integral basis) over the domain of algebraic integers $\mathfrak{o}$ in K if, and only if, $\mathfrak{d}(\Lambda/K)$ is principal.*

A criterion for the existence of a relative integral basis was for the first time given by ARTIN (cf. [1]) in terms of the classical relative discriminant $(\mathfrak{d}(\Lambda/K))$ and of the discriminant α of a K-basis of Λ. The ideal $(\mathfrak{d}(\Lambda/K))\,(\alpha^{-1})$ is the square of an ideal $\mathfrak{a}$ and the required necessary and sufficient condition is that $\mathfrak{a}$ be a principal ideal. We shall see in a consecutive paper (cf. [3]) how this result connects up with our theory. It seems that the new definition of a discriminant is, however, the natural one to use, if one wants to formulate a simple criterion which does not involve explicitly any basis of Λ but only depends on an intrinsic property, and which so allows us to find fairly general classes of extension fields Λ with a relative integral basis (e.g. 3.2., 4.3.). There is no simple property of $(\mathfrak{d}(\Lambda/K))$ qua ideal which would suffice here. Thus it is easy to construct examples of discriminants $\mathfrak{d}(\Lambda/K)$ which are not principal, while the ideal $(\mathfrak{d}(\Lambda/K))$ is principal.

The crux of 2.5. lies in the sufficiency part. For this we require $\mathfrak{d}(\Lambda/K)$ merely to have a representative $\alpha \in K^\times$ mod U_K^2; that α is the discriminant of a free $\mathfrak{o}$-basis of $\mathfrak{Q}$ does not have to be postulated, but is a consequence of the hypothesis.

PROOF of 2.5. The necessity of the condition follows, as already indicated by 2.4.

Assume then $\mathfrak{d}(\Lambda/K)$ to have a representative δ in $K^\times$. There will certainly exist a basis

$$\alpha^{(1)}, \ldots, \alpha^{(n)} \tag{2.5}$$

of Λ/K and an integral ideal $\mathfrak{a}$ in K such that $\beta \in \Lambda$ is an algebraic integer if and only if in the representation

$$\beta = \sum_{i=1}^{n} a^{(i)} \alpha^{(i)} \qquad (a^{(i)} \in K)$$

we have[3])

$$a^{(i)} \in \mathfrak{o} \quad (i < n), \qquad a^{(n)} \in \mathfrak{a}. \tag{2.6}$$

Let α be the discriminant of the basis (2.5). Then for all $\mathfrak{p}$, $\alpha_p \delta_p^{-1} \in \mathsf{K}_p^{\times 2}$ and so $\alpha\delta^{-1} \in J_{\mathsf{K}}^2$. As $\alpha\delta^{-1} \in \mathsf{K}^\times$ we have $\alpha\delta^{-1} \in \mathsf{K}^{\times 2}$, i.e.

$$\delta = \alpha\gamma^2, \qquad \gamma \in \mathsf{K}^\times. \tag{2.7}$$

Let $\mathfrak{p}^r$ be the highest power of the finite prime divisor $\mathfrak{p}$ contained in $\mathfrak{a}$.

$$\alpha_p^{(1)}, \ldots, \alpha_p^{(n)} \tag{2.8}$$

is a basis of A_p/K_p and by (2.6) an element $\beta_p \in A_p$ will lie in $\mathfrak{O}_p$ if and only if in the representation

$$\beta_p = \sum_{i=1}^{n} b^{(i)} \alpha_p^{(i)}, \qquad (b^{(i)} \in \mathsf{K}_p)$$

we have

$$b^{(i)} \in \mathfrak{o}_p \quad (i < n), \qquad b^{(n)} \equiv 0 \pmod{\mathfrak{p}^r}.$$

Let π be any element in $\mathfrak{o}_p$ such that $(\pi) = \mathfrak{p}^r$. Then

$$\alpha_p^{(1)}, \ldots, \alpha_p^{(n-1)}, \pi\alpha_p^{(n)} \tag{2.9}$$

is a basis of $\mathfrak{O}_p$ over $\mathfrak{o}_p$. The discriminant of (2.8) is α_p and so the discriminant of (2.9) is $\alpha_p\pi^2$. By hypothesis on δ, $\delta_p^{-1}\alpha_p\pi^2 \in U_p^2$, and so by (2.7) $\pi^{-1}\gamma_p \in U_p$. But the choice of π among generators of $\mathfrak{p}^r$ was left open, and thus we may take $\pi = \gamma_p$. Hence

$$\alpha_p^{(1)}, \ldots, \alpha_p^{(n-1)}, \gamma_p\alpha_p^{(n)}$$

is an $\mathfrak{o}_p$-basis of $\mathfrak{O}_p$, for all $\mathfrak{p}$, and thus

$$\alpha^{(1)}, \ldots, \alpha^{(n-1)}, \gamma\alpha^{(n)}$$

is an integral basis of $\mathfrak{O}$ over $\mathfrak{o}$.

In [8] I. SCHUR gave a surprisingly simple proof of the congruence property

$$D \equiv 0 \text{ or } 1 \pmod 4$$

of absolute discriminants in the rational field, originally discovered by STICKELBERGER (cf. [9]). To express the non-rational analogue of this result in a simple manner we write for any idèles $\mathfrak{m}$, $\mathfrak{n}$ in J_{K} and any integral ideal $\mathfrak{a}$ in K, $\mathfrak{m} \equiv \mathfrak{n}^2 \pmod{\mathfrak{a}}$ if, when $\mathfrak{a} = \prod(\mathfrak{p})^{r_\mathfrak{p}}$ is the decomposition of $\mathfrak{a}$ into distinct prime power ideals, then $\mathfrak{m}_p - \mathfrak{n}_p^2 \equiv 0 \pmod{\mathfrak{p}^{r_\mathfrak{p}}}$, whenever $r_\mathfrak{p} > 0$. We shall say the discriminant $\mathfrak{d}$ is quadratic residue mod $\mathfrak{a}$ if for some representative idèle $\mathfrak{m}$ of $\mathfrak{d}$ (and so for all representative idèles of $\mathfrak{d}$), the congruence $\mathfrak{m} \equiv \mathfrak{n}^2 \pmod{\mathfrak{a}}$ has a solution.

2.6. THEOREM. *Every discriminant is a quadratic residue* mod 4.

PROOF. It will suffice to show that every local discriminant $\mathfrak{d}(A_p/\mathsf{K}_p)$ is a quadratic residue mod $\mathfrak{p}^{2r}$, whenever $\mathfrak{p}$ lies above 2 and $\mathfrak{p}^{2r}$ is the precise power of $\mathfrak{p}$ dividing 4. Moreover by (1.3) we may assume A_p to be a field. But in this case SCHUR'S proof applies almost without change.

[3]) This follows from the fundamental structure theorem on $\mathfrak{o}$-modules. See [3] and the literature quoted there.

§ 3. Quadratic Discriminants

Let $\Omega = \mathsf{K}(\sqrt{\alpha})$ be a quadratic field (over K); $\mathfrak{d}(\Omega/\mathsf{K})$ is called a *quadratic discriminant*. We shall determine the local discriminants. Here we may assume that $\alpha \in \mathfrak{o}^\times$, and, for a fixed finite prime divisor p, also $\alpha \not\equiv 0 \pmod{p^2}$. δ_p will stand for a suitable representative of $\mathfrak{d}(\Omega_p/\mathsf{K}_p)$ in $\mathsf{K}_p^\times$.

3.1. THEOREM. (a) *Let p be a finite prime divisor not lying above 2. Then* $\delta_p = \alpha_p$.

(b) *Let p be a finite prime divisor lying above 2.*

(i) *If* $\alpha \equiv 0 \pmod{p}$ *then* $\delta_p = 4_p \alpha_p$.

(ii) *If* $\alpha_p \in U_p$ *and if s is the greatest positive integer such that firstly*

$$4 \equiv 0 \pmod{p^{2s}},$$

and in the second place

$$\exists\, \gamma_p \in U_p \quad \text{with} \quad \alpha_p \equiv \gamma_p^2 \pmod{p^{2s}},$$

then

$$\delta_p = (2_p \pi^{-1})^2 \alpha_p, \quad \text{where} \quad \pi \in \mathfrak{o}_p^\times, \quad (\pi) = p^s.$$

(c) *Let p be an infinite real prime divisor. Then* $\delta_p = \alpha_p$.

The corresponding results for the ideal $(\mathfrak{d}(\Omega/\mathsf{K}))$ are of course classical.

PROOF. If $\alpha \in \mathsf{K}_p^{\times 2}$ then $\mathfrak{d}(\Omega_p/\mathsf{K}_p) = 1$. But having assumed that $\alpha_p \not\equiv 0 \pmod{p^2}$ we then also have $\alpha_p \in U_p^2$ and so $\delta_p = \alpha_p$. Henceforth we assume that $\alpha_p \notin \mathsf{K}_p^{\times 2}$.

(a) $1_p, \sqrt{\alpha_p}$ is a basis of $\mathfrak{Q}_p$ with discriminant $4_p \alpha_p$; as $4_p \in U_p^2$ we have $\delta_p = \alpha_p$.

(b) If first $\alpha_p \equiv 0 \pmod{p}$ then we see as under (a) that $1_p, \sqrt{\alpha_p}$ is a basis of $\mathfrak{Q}_p$ with discriminant $4_p \alpha_p$. Assume now that $\alpha_p \in U_p$. If s, γ_p and π satisfy the conditions stated then $1_p, (\gamma_p + \sqrt{\alpha_p})\pi^{-1}$ is a basis of $\mathfrak{Q}_p$ with discriminant $\delta_p = (2_p \pi^{-1})^2 \alpha_p$.

(c) If $\alpha_p > 0$ we have already seen that δ_p may be taken as any positive number. If $\alpha_p < 0$ then $1_p, (1_p + \sqrt{\alpha_p})\, 2^{-1}$ is a basis of Ω_p with discriminant α_p.

From 3.1 we see in particular that if p is a prime divisor in K lying above 2, and if p^r is the precise power of p entering the prime decomposition of (2), then for each representative δ of $\mathfrak{d}(\Omega/\mathsf{K})$ in J_K there will exist an element $\beta_p \in \mathfrak{o}_p^\times$ such that $\delta_p - \beta_p^2 \equiv 0 \pmod{p^{2r}}$. It follows that there exists an algebraic integer β in K such that $\delta - \beta^2 \equiv 0 \pmod 4$. This observation leads to an explicit construction of an integral basis whenever $\mathfrak{d}(\Omega/\mathsf{K})$ is principal, i.e. δ is taken as an element of $\mathfrak{o}^\times$. In fact with the previous connotation of β, we get the integral basis $1, (\beta + \sqrt{\delta})/2$.

Another related application of 3.1 gives

3.2. THEOREM. *If α is an algebraic integer in K such that*

(i) *the ideal (α) is square free,*

(ii) *α is prime to 2 and quadratic residue* mod 4,

then the algebraic integers in $\mathsf{K}(\sqrt{\alpha})$ have an integral basis over $\mathfrak{o}$.

In fact by (i) α_p satisfies the hypothesis $\alpha_p \equiv 0 \pmod{p^2}$ simultaneously for all finite prime divisors p. We may then apply 3.1 and conclude that under hypothesis (ii) α is a representative of $\mathfrak{d}(\Omega|\mathsf{K})$. 3.2 now follows by 2.5.

Another corollary of 3.1 is

3.3. *Let S be a set of prime divisors in K, containing all but a finite number of these. If $\mathfrak{d} \in J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2$ then there exists at most one quadratic field Ω with $\mathfrak{d}_p = \mathfrak{d}(\Omega_p|\mathsf{K}_p)$ for all $p \in S$.*

Proof. Assume $\mathfrak{d}(\Omega'_p|\mathsf{K}_p) = \mathfrak{d}(\Omega_p|\mathsf{K}_p)$ for all $p \in S$. We shall only consider those prime divisors in S which are finite, and are non ramified in Ω and in Ω'. By 3.1 any such prime divisor p will split in Ω if, and only if, $\mathfrak{d}(\Omega_p|\mathsf{K}_p) = 1$. Apply the same criterion to Ω'. Thus with a possible finite number of exceptions the finite prime divisors in K which split in Ω will also split in Ω', and vice versa. This implies $\Omega = \Omega'$.

We now define the mapping

$$\psi\colon\ \mathsf{K}^\times/\mathsf{K}^{\times 2} \to J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2$$

by

$$\psi(\alpha \mathsf{K}^{\times 2}) = \mathfrak{d}\left(\mathsf{K}(\sqrt{\alpha})/\mathsf{K}\right).$$

$\operatorname{Im}\psi$ is thus the set of quadratic discriminants.

We furthermore define the epimorphism

$$\vartheta\colon\ J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2 \to \mathsf{K}^\times/\mathsf{K}^{\times 2}$$

as the composition of the epimorphism $J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2 \to J_{\mathsf{K}}^2 P_{\mathsf{K}}/J_{\mathsf{K}}^2$ with the isomorphism $J_{\mathsf{K}}^2 P_{\mathsf{K}}/J_{\mathsf{K}}^2 \cong P_{\mathsf{K}}/J_{\mathsf{K}}^2 \cap P_{\mathsf{K}} = \mathsf{K}^\times/\mathsf{K}^{\times 2}$. Let δ be a representative in J_{K} of $\mathfrak{d} \in J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2$. If $\mathfrak{d} = \psi(\alpha \mathsf{K}^{\times 2})$ then by 3.1 $\delta_p \alpha_p^{-1} \in \mathsf{K}_p^{\times 2}$ for all p and so $\delta\alpha^{-1} \in J_{\mathsf{K}}^2$. Thus

(3.1) $$\vartheta \circ \psi = \text{identity mapping of } \mathsf{K}^\times/\mathsf{K}^{\times 2}.$$

If $\vartheta(\mathfrak{d}) = \alpha \mathsf{K}^{\times 2}$ then trivially $\alpha\delta^{-1} \in J_{\mathsf{K}}^2$. Hence in the first place δ will be an idèle square in the quadratic field Ω if, and only if, α is an idèle square, i.e. a square in $\Omega^\times$, and so if, and only if, $\Omega \supseteq \mathsf{K}(\sqrt{\alpha})$. Moreover, denoting by ϑ_2 the restriction of ϑ to $\operatorname{Im}\psi$, we see by (3.1) that

(3.2) $$\psi \circ \vartheta_2 = \text{identity mapping of } \operatorname{Im}\psi.$$

We shall say that the element $\mathfrak{d} \in J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2$ is a square in Ω if some representative δ in J_{K} (and so each of its representatives) is an idèle square in Ω.

From the preceding discussion and from 3.3 we now have, allowing K to be counted as a quadratic field,

3.4. Theorem. *Distinct quadratic fields have distinct discriminants. In particular K is the only quadratic field with discriminant 1.*

If $\Omega \neq \mathsf{K}$ is a quadratic field then each of the following properties characterises $\mathfrak{d}(\Omega|\mathsf{K})$ uniquely in the set of all quadratic discriminants different from 1.

(i) *$\mathfrak{d}(\Omega|\mathsf{K})$ is a square in Ω.*

(ii) *$\mathfrak{d}(\Omega_p|\mathsf{K}_p) = 1$ whenever p splits in Ω.*

Moreover we get

3.5. (i) *For each element* $\mathfrak{d} \in J_K^2 P_K/U_K^2$, $\mathfrak{d} \notin J_K^2/U_K^2$ *there exists one and only one quadratic field* Ω *in which* $\mathfrak{d}$ *is a square.*

(ii) *For each element* $\mathfrak{d} \in J_K^2 P_K/U_K^2$ *there exists one and only one quadratic discriminant* $\mathfrak{d}_1$ *such that* $\mathfrak{d} J_K^2 = \mathfrak{d}_1 J_K^2$.

(iii) *If* $\mathfrak{d} \notin J_K^2/U_K^2$, *if* Ω *is the field determined in* (i) *and* $\mathfrak{d}_1$ *the discriminant obtained in* (ii) *then* $\mathfrak{d}_1 = \mathfrak{d}(\Omega/K)$.

The mapping $\mathfrak{m} \to \mathfrak{m}^2 (\mathfrak{m} \in J_K)$ gives rise to an isomorphism

$$\tau\colon J_K/U_K \to J_K^2/U_K^2. \tag{3.3}$$

If $\mathfrak{d}_1, \mathfrak{d}_2$ are quadratic discriminants then by 3.5 (ii) there exists a unique quadratic discriminant $(\mathfrak{d}_1 \mathfrak{d}_2)^\times$ and a unique ideal $\mathfrak{a}(\mathfrak{d}_1, \mathfrak{d}_2)$ such that

$$\mathfrak{d}_1 \mathfrak{d}_2 = \tau\, \mathfrak{a}(\mathfrak{d}_1, \mathfrak{d}_2) \cdot (\mathfrak{d}_1 \mathfrak{d}_2)^\times.$$

The function $\mathfrak{a}(\mathfrak{d}_1, \mathfrak{d}_2)$ is a factor set of $J_K^2 P_K/J_K^2$ in the ideal group J_K/U_K. From 3.1 we deduce

3.6. *If* $\mathfrak{d}_1, \mathfrak{d}_2$ *are quadratic discriminants and if the ideals* $(\mathfrak{d}_1), (\mathfrak{d}_2)$ *are coprime then* $\mathfrak{d}_1 \mathfrak{d}_2$ *is a quadratic discriminant. In particular the non ramified quadratic discriminants — characterised by* $(\mathfrak{d}) = (1)$ *— form a group.*

In conclusion we establish an ideal theoretic criterion for the existence of an integral basis in quadratic extensions due to H. B. MANN (cf. [7]).

3.7. *The algebraic integers in a quadratic extension* Ω *of* K *have an integral basis over* $\mathfrak{o}$ *if, and only if,* $(\mathfrak{d}(\Omega/K)) = (\beta)$ *where* $\Omega = K(\sqrt{\beta})$.

PROOF. We may assume $\Omega \neq K$. If first

$$\mathfrak{d}(\Omega/K) = \beta\, U_K^2, \qquad \beta \in K^\times, \tag{3.4}$$

then trivially

$$(\beta) = (\mathfrak{d}(\Omega/K)) \tag{3.5}$$

and by 3.4

$$\Omega = K(\sqrt{\beta}). \tag{3.6}$$

For the converse let δ be a representative of $\mathfrak{d}(\Omega/K)$. By (3.5) $\delta\beta^{-1} \in U_K$ and by (3.6) $\delta\beta^{-1} \in J_K^2$ whence $\delta\beta^{-1} \in U_K^2$, i.e. (3.4) is valid.

The question of the existence of quadratic extensions with relative integral basis will in a more general context be dealt with elseweher.

§ 4. The Discriminant Field

By 3.5 there exists for every finite extension Λ of K a unique quadratic field Ω called the *discriminant field* of Λ such that

$$\mathfrak{d}(\Lambda/K)\, J_K^2 = \mathfrak{d}(\Omega/K)\, J_K^2. \tag{4.1}$$

There thus exists an ideal $\mathfrak{a} = \mathfrak{a}_\Lambda$ such that

$$\mathfrak{d}(\Lambda/K) = \mathfrak{d}(\Omega/K) \cdot \tau\, \mathfrak{a}_\Lambda \tag{4.2}$$

where τ is the isomorphism defined in (3.3). For the corresponding ideals we get then

$$(\mathfrak{d}(\Lambda/\mathsf{K})) = (\mathfrak{d}(\Omega/\mathsf{K}))\,\mathfrak{a}_\Lambda^2. \tag{4.3}$$

For any finite prime divisor p not lying above 2 we have $(\mathfrak{d}(\Lambda_p/\mathsf{K}_p)) = p^r$ $(r \geqq 0)$ and $(\mathfrak{d}(\Omega_p/\mathsf{K}_p)) = p^s$, $s = 0$, or $= 1$. It follows that $\mathfrak{a}_p = p^t$ $(t \geqq 0)$. An analogous result can be established from 3.1 and from the generalisation of STICKELBERGER's theorem (cf. 2.6) when p lies above 2. We thus have[4])

4.1. THEOREM. *$\mathfrak{a}_\Lambda$ is always an integral ideal.*

Let $\bar{\Lambda}$ be the least normal field (over K) containing Λ. If $\vartheta(\mathfrak{d}(\Lambda/\mathsf{K})) = \alpha \mathsf{K}^{\times 2}$ then for each p, α_p is the discriminant of some basis of Λ_p/K_p and so $\alpha_p \in \bar{\Lambda}_p^{\times 2}$. Hence $\alpha \in J_\Lambda^2$, and so $\mathsf{K}(\sqrt{\alpha}) \subseteq \bar{\Lambda}$. We have shown that

4.2. *The discriminant field of Λ is contained in the least normal field over K containing Λ.*

Assume now Λ to be normal of odd degree over K. Then K is the discriminant field of Λ and so $\mathfrak{d}(\Lambda/\mathsf{K}) \in J_\mathsf{K}^2/U_\mathsf{K}^2$. If moreover Λ/K is non ramified then $\mathfrak{d}(\Lambda/\mathsf{K}) \in U_\mathsf{K}/U_\mathsf{K}^2$, and so $\mathfrak{d}(\Lambda/\mathsf{K}) = 1$. By 2.5 we conclude

4.3. THEOREM. *In every normal, non ramified extension Λ of odd degree over K, the integers have a free module basis over the integers in K.*

Note that for quadratic fields Ω, $\mathfrak{d}(\Omega_p/\mathsf{K}_p) \in \mathsf{K}_p^{\times 2}/U_p^2$ implies $\mathfrak{d}(\Omega_p/\mathsf{K}_p) = 1$. Thus

4.4. THEOREM. *$\mathfrak{d}(\Lambda_p/\mathsf{K}_p) \in \mathsf{K}_p^{\times 2}/U_p^2$ if, and only if, p splits in the discriminant field of Λ.*

Let p be a real infinite prime. The value ± 1 of the functions $\operatorname{sgn}_p(\mathfrak{m})$ depends solely on the class of $\mathfrak{m} \bmod J_\mathsf{K}^2$. We may thus consider sgn_p as a class function mod J_K^2. The same is trivially true if p is complex. The ordered set of numbers $\operatorname{sgn}_p(\mathfrak{d})$ as p runs through the infinite primes is the *signature* of the discriminant $\mathfrak{d}$. From 3.1 we get

4.5. THEOREM. *Let p be a real infinite prime. If Λ_p is the sum of r_1 copies of the field of real numbers and of r_2 copies of the field of complex numbers then*

$$\operatorname{sgn}_p(\mathfrak{d}(\Lambda/\mathsf{K})) = (-1)^{r_2}.$$

As an application of the notion of a signature we prove

4.6. THEOREM. *The ideal class of $(\mathfrak{d}(\Lambda/\mathsf{K}))$ in the narrow sense, i.e. modulo the totally positive principal ideals is a square if the signature of $\mathfrak{d}(\Lambda/\mathsf{K})$ coincides with the signature of some unit in $\mathsf{K}^\times$.*

PROOF. Let $\mathfrak{m}^2\alpha$ be a representative idèle of $\mathfrak{d}(\Lambda/\mathsf{K})$, $\alpha \in P_\mathsf{K}$. The signature of $\mathfrak{d}(\Lambda/\mathsf{K})$ is the signature of α; but (α) is a totally positive principal ideal if, and only if, the signature of α coincides with the signature of some unit in $\mathsf{K}^\times$.

HERBRAND (cf. [6]) proved the following theorem for metacyclic extensions and conjectured its validity in general.

[4]) For the rational case see [4], S. 371.

4.7. THEOREM. *The ideal* $(\mathfrak{d}(\Lambda/\mathsf{K}))$, $(\Lambda/\mathsf{K}$ *normal*$)$ *can be written in the form* $\mathfrak{a}^2(\alpha)$, $\alpha \in \mathsf{K}^\times$ *where*

(i) $\alpha \equiv 1 \pmod{\mathfrak{b}}$, $\mathfrak{b}$ *the greatest divisor of* 4 *prime to* $(\mathfrak{d}(\Lambda/\mathsf{K}))$.

(ii) $\alpha_p > 0$ *for each real prime divisor* p, *except when* Λ_p *is a direct sum of copies of the field of complex numbers and* $(\Lambda:\mathsf{K}) \equiv 2 \pmod 4$.

4.7 does in fact follow in complete generality by 2.6 and 4.5. (i) is also true when Λ/K is not normal, while in place of the congruence in (ii) we have $r_2 \equiv 1 \pmod 2$.

In conclusion we consider cubic fields over K. Such a field is either not normal or it is cyclic.

4.8. THEOREM. *A cubic field* Λ *is cyclic if, and only if,* $\mathfrak{d}(\Lambda/\mathsf{K}) \in J_\mathsf{K}^2/U_\mathsf{K}^2$ (i.e. "$\mathfrak{d}(\Lambda/\mathsf{K})$ *is a square*").

PROOF. If Λ is cyclic then by 4.2 its discriminant field is K and so $\mathfrak{d}(\Lambda/\mathsf{K})$ is a square.

Assume Λ not to be normal. Let $\bar{\Lambda}$ be the normal field of degree 6 containing Λ. All conjugacy classes in the Galois group of $\bar{\Lambda}/\mathsf{K}$ give values of the Frobenius symbols for some non ramified finite prime divisor $\mathfrak{p}$. We may thus choose $\mathfrak{p}$ so that $\Lambda_\mathfrak{p}$ is the direct sum of $\mathsf{K}_\mathfrak{p}$ and of a quadratic field $\Omega_\mathfrak{p}$. Hence $\mathfrak{d}(\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}) = \mathfrak{d}(\Omega_\mathfrak{p}/\mathsf{K}_\mathfrak{p})$. But $\mathfrak{d}(\Omega_\mathfrak{p}/\mathsf{K}_\mathfrak{p})$ cannot be a square, and so $\mathfrak{d}(\Lambda/\mathsf{K})$ is not a square.

References

[1] ARTIN, E.: Questions de la base minimale dans la théorie des nombres algébriques. Centre Nat. Rech. Sci. XXIV (Colloq. Int., Paris, 1949), 19–20. — [2] CHEVALLEY, C.: La theorie du corps de classes. Ann. Math. (2) **41**, 394–418 (1940). — [3] FRÖHLICH, A.: Ideals in an extension field as modules over the algebraic integers in a finite number field. Math. Z. **74**, 29–38 (1960). — [4] HASSE, H.: Zahlentheorie. Berlin 1949. — [5] HECKE, E.: Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig 1923 (New York 1948). — [6] HERBRAND, J.: Une propriété du discriminant des corps algébriques. Ann. École normale (3) **49**, 105–112 (1932). — [7] MANN, H.B.: On integral bases. Proc. Amer. Math. Soc. **9**, 167–172 (1958). — [8] SCHUR, I.: Elementarer Beweis eines Satzes von L. STICKELBERGER. Math. Z. **29**, 464–465 (1929). — [9] STICKELBERGER, L.: Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper. Verh. I. Int. Math. Kongr. 1897, S. 182–193.

King's College, London W.C. 1 (England)

(Eingegangen am 15. September 1959)

Fröhlich, A.
Math. Zeitschr. 74, 29—38 (1960)

Ideals in an extension field as modules over the algebraic integers in a finite number field

By
Albrecht Fröhlich

In the preceding paper [4] the concept of an "absolute" discriminant of a finite algebraic extension Λ was extended from the rational field to an arbitrary finite number field K as base field. In the present [1]) note we shall discuss the structure of (fractional) ideals in Λ as modules over the ring $\mathfrak{o}$ of algebraic integers in K on the basis of the theory developed in [4].

With an ideal $\mathfrak{A}$ in the extension field Λ there will be associated three invariants. The *relative norm* $N_{\Lambda/\mathsf{K}}\mathfrak{A}$ is in the usual manner defined as an ideal in K. It is the "order" of the quotient module $\mathfrak{O}-\mathfrak{A}$ considered as an $\mathfrak{o}$-module whenever $\mathfrak{A}$ is integral; here $\mathfrak{O}$ is the ring of algebraic integers in Λ. This property and the multiplicative law $N_{\Lambda/\mathsf{K}}(\mathfrak{A}\mathfrak{B})=N_{\Lambda/\mathsf{K}}(\mathfrak{A})\,N_{\Lambda/\mathsf{K}}(\mathfrak{B})$ characterise the relative norm uniquely.

A new invariant to be introduced here is the *discriminant* $\mathfrak{d}(\mathfrak{A})$ of $\mathfrak{A}$ in K, which is a generalisation of the discriminant of a basis of $\mathfrak{A}$ when K is the rational field. $\mathfrak{d}(\mathfrak{A})$ is a class of idèles modulo the unit idèle squares; if $\mathfrak{A}=\mathfrak{O}$, it is the discriminant of Λ/K defined in the earlier paper. We shall obtain the non-rational analogue to the rational formula $|N_{\Lambda/\mathsf{K}}\mathfrak{A}|=+\sqrt{(D(\mathfrak{A})/D)}$ for the absolute norm $|N_{\Lambda/\mathsf{K}}\mathfrak{A}|$, the absolute discriminant D and the discriminant $D(\mathfrak{A})$ of a basis of $\mathfrak{A}$. In particular it will follow that $\mathfrak{d}(\mathfrak{A})$ and $N_{\Lambda/\mathsf{K}}\mathfrak{A}$ determine each other uniquely (cf. 2.5).

The relative norm and the discriminant are arithmetical invariants depending on the properties of $\mathfrak{A}$ as an ideal in Λ. The structure of $\mathfrak{A}$ qua $\mathfrak{o}$-module is however, for given degree $(\Lambda:\mathsf{K})$, uniquely determined by a *module-invariant* $C(\mathfrak{A})$ which is an ideal class in K. Such an invariant can be defined for any finitely generated torsion free $\mathfrak{o}$-module, whether embedded as an ideal in some extension field Λ of K, or not; the definition of $C(\mathfrak{A})$ thus will not depend on the arithmetic in Λ. We shall however show that in the given situation the actual value of $C(\mathfrak{A})$ can be determined in terms of the relative norm and also in terms of the discriminant (cf. 2.3, 2.8). In particular we shall obtain a necessary and sufficient arithmetical criterion for $\mathfrak{A}$ to have a free $\mathfrak{o}$-basis (cf. 2.4); for $\mathfrak{A}=\mathfrak{O}$ this had been done already in [4]. The results obtained lead then to a formula for the number of ideal classes C in K which are module-invariants for ideals in a given field Λ (cf. 2.11). From this we shall deduce a new characterisation of the absolute class field (cf. 2.12).

[1]) As in [4] (see footnote 1) we restrict ourselves here to number fields, leaving the obvious generalisations to the reader.

The discussion of the invariants of ideals forms the contents of § 2. In § 1 the theory of finitely generated, torsion free modules over the ring $\mathfrak{o}$ of algebraic integers in K will be presented. The contents of § 1 is not essentially new; the subject has been dealt with in various forms by STEINITZ [8], SCHUR [7], KRULL [6], FRANZ [3], CHEVALLEY [2] and KAPLANSKY [5]. Our approach will differ in detail from that in the previous literature; it has been chosen with the application to the module theory of ideals in mind.

§ 1. Module Invariants

NOTATION. In any integral domain R, $R^\times$ is the semigroup of non zero elements. K is a finite algebraic number field, and $\mathfrak{o}$ is the domain of algebraic integers in K. $\mathsf{K}_\mathfrak{p}$ is the completion of K for a prime divisor $\mathfrak{p}$ in K; if $\mathfrak{p}$ is finite $\mathfrak{o}_\mathfrak{p}$ is the ring of valuation integers in $\mathsf{K}_\mathfrak{p}$ and $U_\mathfrak{p}$ the group of units; if $\mathfrak{p}$ is infinite, $\mathfrak{o}_\mathfrak{p}=\mathsf{K}_\mathfrak{p}$ and $U_\mathfrak{p}=\mathsf{K}_\mathfrak{p}^\times$. J_K is the idèle group of K and U_K the group of unit idèles i.e. $U_\mathsf{K}=\prod U_\mathfrak{p}$; P_K is the group of principal idèles. Thus the ideal group can be identified with $J_\mathsf{K}/U_\mathsf{K}$ and the ideal class group with $J_\mathsf{K}/P_\mathsf{K}U_\mathsf{K}$.

We consider finitely generated, torsion free $\mathfrak{o}$-modules M, briefly referred to as "$\mathfrak{o}$-modules". For any such module the tensor product

$$V=M\otimes_\mathfrak{o}\mathsf{K} \tag{1.1}$$

is a K-space whose K-rank we denote by $(V:\mathsf{K})$. $(V:\mathsf{K})$ is finite. The $\mathfrak{o}$-rank $(M:\mathfrak{o})$ of M is then defined by

$$(M:\mathfrak{o})=(V:\mathsf{K}). \tag{1.2}$$

If M is a free $\mathfrak{o}$-module this definition agrees with that in terms of a free basis.

We shall identify $M=M\otimes_\mathfrak{o}\mathfrak{o}$ and consider M as embedded in V by means of the natural injection $\mathfrak{o}\to\mathsf{K}$. From the rank-properties of K-spaces we get formuli for the ranks of the direct sum $M_1\dotplus M_2$ and the tensor product $M_1\otimes_\mathfrak{o}M_2$ of two $\mathfrak{o}$-modules:

$$(M_1\dotplus M_2:\mathfrak{o})=(M_1:\mathfrak{o})+(M_2:\mathfrak{o}), \tag{1.3}$$

$$(M_1\otimes_\mathfrak{o}M_2:\mathfrak{o})=(M_1:\mathfrak{o})\,(M_2:\mathfrak{o}). \tag{1.4}$$

The rank is of course invariant under $\mathfrak{o}$-isomorphism. If $(M:\mathfrak{o})=0$ then M is the zero module; thus this rank equation determines M uniquely. If $(M:\mathfrak{o})=1$ we may assume $V=\mathsf{K}$. M is then an ideal in K in the sense of algebraic number theory. Two ideals $\mathfrak{a}$ and $\mathfrak{b}=\mathfrak{a}(\gamma)$, with $\gamma\in\mathsf{K}^\times$, are $\mathfrak{o}$-isomorphic under the mapping $\alpha\to\alpha\gamma$. Conversely an $\mathfrak{o}$-isomorphism $\mathfrak{a}\cong\mathfrak{b}$ of ideals can be extended uniquely to a K-endomorphism of K which is not null, and hence is of form $\varkappa\to\varkappa\gamma$, $\gamma\in\mathsf{K}^\times$. Thus $\mathfrak{b}=\mathfrak{a}(\gamma)$. We have seen that

1.1. *Two ideals in* K *are* $\mathfrak{o}$*-isomorphic if, and only if, they lie in the same absolute ideal class.*

We shall now consider $\mathfrak{o}$-modules of fixed rank $n>0$ embedded in a K-space V of rank n. For every such module M and every prime divisor $\mathfrak{p}$ in K we put

$$M \otimes_{\mathfrak{o}} \mathfrak{o}_{\mathfrak{p}} = M_{\mathfrak{p}}. \tag{1.5}$$

Furthermore we write

$$V \otimes_{\mathsf{K}} \mathsf{K}_{\mathfrak{p}} = V_{\mathfrak{p}}. \tag{1.6}$$

The injection $\mathfrak{o}_{\mathfrak{p}} \to \mathsf{K}_{\mathfrak{p}}$ leads in view of the isomorphisms

$$V_{\mathfrak{p}} = (M \otimes_{\mathfrak{o}} \mathsf{K}) \otimes_{\mathsf{K}} \mathsf{K}_{\mathfrak{p}} \cong M \otimes_{\mathfrak{o}} (\mathsf{K} \otimes_{\mathsf{K}} \mathsf{K}_{\mathfrak{p}}) \cong M \otimes_{\mathfrak{o}} \mathsf{K}_{\mathfrak{p}}$$

to a natural embedding of $M_{\mathfrak{p}}$ in $V_{\mathfrak{p}}$. We have

$$(V_{\mathfrak{p}} : \mathsf{K}_{\mathfrak{p}}) = (V : \mathsf{K}) \tag{1.7}$$

and

$$(M_{\mathfrak{p}} : \mathfrak{o}_{\mathfrak{p}}) = (M : \mathfrak{o}). \tag{1.8}$$

Let M, N be $\mathfrak{o}$-modules in V of rank n. Then $M_{\mathfrak{p}}$, $N_{\mathfrak{p}}$ are free $\mathfrak{o}_{\mathfrak{p}}$-modules of rank n and are thus $\mathfrak{o}_{\mathfrak{p}}$-isomorphic. Every $\mathfrak{o}_{\mathfrak{p}}$-isomorphism $\sigma_{\mathfrak{p}}$: $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ can be extended in a unique manner to a $\mathsf{K}_{\mathfrak{p}}$-endomorphism $\bar{\sigma}_{\mathfrak{p}}$: $V_{\mathfrak{p}} \to V_{\mathfrak{p}}$; $\bar{\sigma}_{\mathfrak{p}}$ is a $\mathsf{K}_{\mathfrak{p}}$-automorphism. Hence its determinant $|\bar{\sigma}_{\mathfrak{p}}|$ is not zero. Moreover this determinant solely depends on M and N, apart from a unit factor. The class of $|\bar{\sigma}_{\mathfrak{p}}|$ in $\mathsf{K}_{\mathfrak{p}}^{\times}/U_{\mathfrak{p}}$, i.e. the local ideal generated by $|\bar{\sigma}_{\mathfrak{p}}|$ is thus uniquely determined by the two modules, and will be denoted by $[M:N]_{\mathfrak{p}}$. From the definition we have

$$[M:M]_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}, \qquad [M:L]_{\mathfrak{p}} = [M:N]_{\mathfrak{p}}\,[N:L]_{\mathfrak{p}}. \tag{1.9}$$

Moreover if $M_{\mathfrak{p}} \supseteqq N_{\mathfrak{p}}$ then $|\bar{\sigma}_{\mathfrak{p}}| \in \mathfrak{o}_{\mathfrak{p}}^{\times}$, and so

$$[M:N]_{\mathfrak{p}} \subseteqq \mathfrak{o}_{\mathfrak{p}} \quad \text{if} \quad M_{\mathfrak{p}} \supseteqq N_{\mathfrak{p}}. \tag{1.10}$$

M and N being finitely generated $\mathfrak{o}$-modules spanning the same K-space V there will exist non zero integers α, β in $\mathsf{K}^{\times}$ with $\alpha M \subseteqq N$ and $\beta N \subseteqq M$. By (1.10), (1.9),

$$(\alpha_{\mathfrak{p}}^{n})\ [N:M]_{\mathfrak{p}} = [N:M]_{\mathfrak{p}}\,[M:\alpha M]_{\mathfrak{p}} \subseteqq \mathfrak{o}_{\mathfrak{p}},$$
$$(\beta_{\mathfrak{p}}^{n})\ [M:N]_{\mathfrak{p}} = [M:N]_{\mathfrak{p}}\,[N:\beta N]_{\mathfrak{p}} \subseteqq \mathfrak{o}_{\mathfrak{p}}.$$

By (1.9) it follows now from these relations that $[M:N]_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}$ whenever $\alpha_{\mathfrak{p}}$ and $\beta_{\mathfrak{p}}$ lie in $U_{\mathfrak{p}}$. This will be the case for almost all $\mathfrak{p}$. Hence the local ideals $[M:N]_{\mathfrak{p}}$ are the $\mathfrak{p}$-components of a unique ideal $[M:N]$ of K, i.e. of a unique element of $J_{\mathsf{K}}/U_{\mathsf{K}}$. (1.9) then leads to

$$[M:M] = \mathfrak{o}, \qquad [M:L] = [M:N]\,[N:L]. \tag{1.11}$$

If $M = \mathfrak{a}$, $N = \mathfrak{b}$ are two ideals in K then $\mathfrak{a}_{\mathfrak{p}}$, $\mathfrak{b}_{\mathfrak{p}}$ are ideals in $\mathsf{K}_{\mathfrak{p}}$ and the $\mathsf{K}_{\mathfrak{p}}$-automorphism $\bar{\sigma}_{\mathfrak{p}}$ is of the form $\varkappa_{\mathfrak{p}} \to \varkappa_{\mathfrak{p}}\gamma_{\mathfrak{p}}$, $\gamma_{\mathfrak{p}} \in \mathsf{K}_{\mathfrak{p}}^{\times}$. Thus $\mathfrak{b}_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}(\gamma_{\mathfrak{p}})$ and so $(\gamma_{\mathfrak{p}}) = \mathfrak{b}_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}^{-1}$. Therefore

$$[\mathfrak{a}:\mathfrak{b}] = \mathfrak{a}^{-1}\mathfrak{b}. \tag{1.12}$$

We now show, returning to the general case

1.2. *If M and N are $\mathfrak{o}$-isomorphic $\mathfrak{o}$-modules spanning the K-space V then $[M:N]$ is a principal ideal.*

In fact we can extend any $\mathfrak{o}$-isomorphism $\sigma: M \cong N$ in a unique manner to a K-endomorphism $\bar{\sigma}: V \to V$; $\bar{\sigma}$ is a K-automorphism. σ induces a unique $\mathfrak{o}_p$-isomorphism $\sigma_p: M_p \cong N_p$ whose extension $\bar{\sigma}_p$ to V_p is precisely the K_p-automorphism of V_p induced by $\bar{\sigma}$. Hence $|\bar{\sigma}_p| = |\bar{\sigma}|_p$ and so $[M:N]_p$ is the p-component of the principal ideal $(|\bar{\sigma}|)$. Thus $[M:N] = (|\bar{\sigma}|)$.

By 1.2. and (1.11) we see that if M and N are $\mathfrak{o}$-isomorphic and if F and G are free $\mathfrak{o}$-modules spanning V then $[F:M]$ and $[G:N]$ lie in the same ideal class. Any K-basis of V will of course be a free set of $\mathfrak{o}$-generators of a free $\mathfrak{o}$-module F. The ideal-class of the ideals $[F:M]$ will then solely depend on M and will be denoted by $C(M)$. $C(M)$ is an invariant of the isomorphism class of M. In fact every $\mathfrak{o}$-isomorphism $\tau: M \cong M'$ can be extended to a K-isomorphism $\bar{\tau}: M \otimes_{\mathfrak{o}} \mathsf{K} \cong M' \otimes_{\mathfrak{o}} \mathsf{K}$ and for every choice of the free $\mathfrak{o}$-module F in $M \otimes_{\mathfrak{o}} \mathsf{K}$, $\bar{\tau} F$ is a free $\mathfrak{o}$-module in $M' \otimes_{\mathfrak{o}} \mathsf{K}$, and $[F:M] = [\bar{\tau} F: M']$.

For $(M:\mathfrak{o}) = 0$ we define $C(M) = 1$.

1.3. THEOREM. (i) *If $\mathfrak{a}$ is an ideal in K then $C(\mathfrak{a})$ is the ideal class of $\mathfrak{a}$.*

(ii) $C(M_1 \dotplus M_2) = C(M_1)\, C(M_2)$.

(iii) $C(M_1 \otimes_{\mathfrak{o}} M_2) = C(M_1)^{(M_2:\mathfrak{o})}\, C(M_2)^{(M_1:\mathfrak{o})}$.

PROOF. (i) follows by (1.12), which gives $\mathfrak{a} = [\mathfrak{o}:\mathfrak{a}]$.

For (ii) we select free $\mathfrak{o}$-modules F_i of maximal rank in $M_i \otimes_{\mathfrak{o}} \mathsf{K}$. Identifying $(M_1 \dotplus M_2) \otimes_{\mathfrak{o}} \mathsf{K} = M_1 \otimes_{\mathfrak{o}} \mathsf{K} \dotplus M_2 \otimes_{\mathfrak{o}} \mathsf{K}$, we see that $F_1 \dotplus F_2$ is a free $\mathfrak{o}$-module of maximal rank in the direct sum of the K-spaces. The formula

$$[F_1 \dotplus F_2 : M_1 \dotplus M_2]_p = [F_1 : M_1]_p\, [F_2 : M_2]_p$$

leads to an analogous global formula and so to (ii). A similar argument will give (iii).

To derive another characterisation of $C(M)$ we show

1.4. *Every $\mathfrak{o}$-module M of rank $n > 0$ is $\mathfrak{o}$-isomorphic to a direct sum of $n-1$ copies of $\mathfrak{o}$ and of an ideal $\mathfrak{a}$.*

PROOF. We first prove by induction on n that M is $\mathfrak{o}$-isomorphic to a direct sum: $\mathfrak{a}_1 \dotplus \cdots \dotplus \mathfrak{a}_n$ of ideals.

For $n = 1$ this, and in fact the whole of 1.4, is trivial. The step from $n-1$ to n is based on the observation that M contains a basis $v_1, \ldots, v_n$ of $M \otimes_{\mathfrak{o}} \mathsf{K}$. Hence every element $u \in M$ has a unique representation

$$u = \sum_{i=1}^{n} a_i v_i, \qquad a_i \in \mathsf{K}.$$

The mapping $\vartheta: u \to a_n$ is an $\mathfrak{o}$-homomorphism $M \to \mathsf{K}$, and $\operatorname{Im} \vartheta$ must be a finitely generated $\mathfrak{o}$-module in K. As $1 \in \operatorname{Im} \vartheta$, it cannot be of rank 0. Hence

Im $\vartheta = \mathfrak{a}_n$ is an ideal in K. $\mathfrak{a}_n$ is $\mathfrak{o}$-projective whence $M \cong \operatorname{Ker}\vartheta \dotplus \mathfrak{a}_n$. By (1.3) the $\mathfrak{o}$-rank of $\operatorname{Ker}\vartheta$ is $n-1$.

Consider now a direct sum $\mathfrak{a}_1 \dotplus \mathfrak{a}_2$ of two ideals. By 1.1 we may assume these to be integral and coprime. We can then find algebraic integers α_i, β_i, γ_i $(i=1, 2)$ such that $\mathfrak{a}_1 = (\alpha_1, \beta_1)$, $\mathfrak{a}_2 = (\alpha_2, \beta_2)$ and $\gamma_1\beta_1 + \gamma_2\beta_2 = 1$. The mapping ψ: $[\delta_1, \delta_2] \to \gamma_1\delta_1 + \gamma_2\delta_2$ is an $\mathfrak{o}$-epimorphism $\mathfrak{a}_1 \dotplus \mathfrak{a}_2 \to \mathfrak{o}$. As $\mathfrak{o}$ is $\mathfrak{o}$-projective we get $\mathfrak{a}_1 \dotplus \mathfrak{a}_2 \cong \operatorname{Ker}\psi \dotplus \mathfrak{o}$. Here $\operatorname{Ker}\psi$ must be of $\mathfrak{o}$-rank 1, i.e. is an ideal. 1.4 now follows for $n>2$ trivially by induction and by the results already established.

For the ideal $\mathfrak{a}$ occurring in 1.4 we get by 1.3 (ii)

$$C(\mathfrak{a}) = C(M). \tag{1.13}$$

Thus the ideal class of $\mathfrak{a}$ is uniquely determined by M. Assume now that $(M:\mathfrak{o}) = (M':\mathfrak{o}) = n$ and that $C(M) = C(M')$. Then by 1.4 $M \cong F \dotplus \mathfrak{a}$, $M' \cong F' \dotplus \mathfrak{a}'$ where F, F' are free $\mathfrak{o}$-modules of rank $n-1$ and $\mathfrak{a}$, $\mathfrak{a}'$ are ideals. By (1.13) and 1.1 $\mathfrak{a} \cong \mathfrak{a}'$. Trivially $F \cong F'$. Hence $M \cong M'$.

We recapitulate the contents of the preceding discussion.

1.5. Theorem. *The invariant $C(M)$ i.e. the ideal class of the ideals $[F:M]$ is also the unique ideal class of ideals $\mathfrak{a}$ occurring in a decomposition* 1.4 $(M \neq 0)$.

1.6. Theorem. *Two finitely generated, torsion free $\mathfrak{o}$-modules M and N are $\mathfrak{o}$-isomorphic if, and only if,*

$$(M:\mathfrak{o}) = (N:\mathfrak{o}),$$

$$C(M) = C(N).$$

In conclusion recall that if $M = \mathfrak{o} \dotplus \cdots \dotplus \mathfrak{o} \dotplus \mathfrak{a}$, then $C(M) = C(\mathfrak{a})$. Thus

1.7. Theorem. *For given $n>0$ and for a given ideal class C in* K *there exists an $\mathfrak{o}$-module M with*

$$(M:\mathfrak{o}) = n,$$

$$C(M) = C.$$

Both for the direct sum and for the tensor product we have found formuli expressing the $\mathfrak{o}$-rank and the invariant C in terms of the component modules [cf. (1.3), (1.4) and theorem 1.3]. For completeness sake similar expressions will be derived for the $\mathfrak{o}$-module $HOM_{\mathfrak{o}}(M, N)$ which is certainly torsion free, whenever N is torsion free.

Consider first of all ideals $\mathfrak{a}$, $\mathfrak{b}$. Every $\mathfrak{o}$-homomorphism ϑ: $\mathfrak{a} \to \mathfrak{b}$ can be extended in a unique manner to a K-endomorphism of K and is thus of the form $\alpha \to \alpha\gamma$, where $\gamma = \gamma_\vartheta$ is a number in K determined by ϑ. As $\alpha\gamma \in \mathfrak{b}$ for all $\alpha \in \mathfrak{a}$ we must have $\gamma \in \mathfrak{a}^{-1}\mathfrak{b}$. The mapping $\vartheta \to \gamma_\vartheta$ is clearly a homomorphism, its kernel is the null mapping. Moreover $\alpha \to \alpha\gamma$ is a homomorphism $\mathfrak{a} \to \mathfrak{b}$ whenever $\gamma \in \mathfrak{a}^{-1}\mathfrak{b}$. Thus the mapping $\vartheta \to \gamma_\vartheta$ is an isomorphism

$$HOM_{\mathfrak{o}}(\mathfrak{a}, \mathfrak{b}) \cong \mathfrak{a}^{-1}\mathfrak{b}. \tag{1.14}$$

If now M is the direct sum of ideals $\mathfrak{a}_i$, and N is the direct sum of ideals $\mathfrak{b}_j$ then $HOM_{\mathfrak{o}}(M, N)$ is isomorphic to the direct sum of the $\mathfrak{o}$-modules $HOM_{\mathfrak{o}}(\mathfrak{a}_i, \mathfrak{b}_j)$. By (1.14), it is finitely generated; more precisely we get

$$(HOM_{\mathfrak{o}}(M, N):\mathfrak{o}) = (M:\mathfrak{o})\,(N:\mathfrak{o}). \tag{1.15}$$

Taking M, N in a decomposition 1.4 we obtain by (1.14)

1.8. THEOREM.

$$C(HOM_{\mathfrak{o}}(M, N)) = C(M)^{-(N:\mathfrak{o})}\, C(N)^{(M:\mathfrak{o})}.$$

§ 2. Ideals

In the present section we consider a finite algebraic extension Λ of K, whose domain of algebraic integers we denote by $\mathfrak{O}$. With every ideal $\mathfrak{A}$ in Λ there is associated as an "arithmetical" invariant the relative norm $N_{\Lambda/\mathsf{K}}\mathfrak{A}$, which is an ideal in K, i.e. an element of $J_{\mathsf{K}}/U_{\mathsf{K}}$. Moreover $\mathfrak{A}$ has in K the *module invariant* $C(\mathfrak{A})$, i.e. the absolute ideal class in K associated by § 1 with the $\mathfrak{o}$-module $\mathfrak{A}$. $C(\mathfrak{A})$ is thus an element of $J_{\mathsf{K}}/P_{\mathsf{K}}U_{\mathsf{K}}$. For the $\mathfrak{o}$-rank of $\mathfrak{A}$ we always have

$$(\mathfrak{A}:\mathfrak{o}) = (\Lambda:\mathsf{K}).$$

Hence $C(\mathfrak{A})$ determines $\mathfrak{A}$ uniquely to within $\mathfrak{o}$-isomorphism. For the ideals $\mathfrak{A}$, $\mathfrak{B}$ in Λ we have $C(\mathfrak{A}) = C(\mathfrak{B})$ if, and only if, there exists a K-automorphism of Λ considered as a K-space, which maps $\mathfrak{A}$ onto $\mathfrak{B}$.

We shall now define a third invariant $\mathfrak{d}(\mathfrak{A})$ of $\mathfrak{A}$ in K, the *discriminant of* $\mathfrak{A}$. $\mathfrak{d}(\mathfrak{A})$ is an element of $J_{\mathsf{K}}/U_{\mathsf{K}}^2$. We first note that for every prime divisor $\mathfrak{p}$ in K, $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{A} \otimes_{\mathfrak{o}} \mathfrak{o}_{\mathfrak{p}}$ is a free $\mathfrak{o}_{\mathfrak{p}}$-module of $\mathfrak{o}_{\mathfrak{p}}$-rank $(\Lambda:\mathsf{K})$. The discriminant of a free $\mathfrak{o}_{\mathfrak{p}}$-basis of $\mathfrak{A}_{\mathfrak{p}}$ is a non zero element of $\mathsf{K}_{\mathfrak{p}}$, uniquely determined mod $U_{\mathfrak{p}}^2$ by $\mathfrak{A}_{\mathfrak{p}}$. Denote by $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{A})$ the class of such discriminants mod $U_{\mathfrak{p}}^2$. $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{A})$ is thus an element of $\mathsf{K}_{\mathfrak{p}}^{\times}/U_{\mathfrak{p}}^2$. For all but a finite number of finite prime divisors $\mathfrak{p}$, $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{O}_{\mathfrak{p}}$ and so $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{A}) = \mathfrak{d}_{\mathfrak{p}}(\mathfrak{O})$. Here $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{O})$ coincides with the local discriminant $\mathfrak{d}(\Lambda_{\mathfrak{p}}/\mathsf{K}_{\mathfrak{p}})$ defined in [4]. Thus if $\mathfrak{p}$ is not a divisor of the ideal $(\mathfrak{d}(\Lambda/\mathsf{K}))$, $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{O})$ will lie in $U_{\mathfrak{p}}/U_{\mathfrak{p}}^2$. We conclude that for all but a finite number of prime divisors $\mathfrak{p}$, we have $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{A}) \in U_{\mathfrak{p}}/U_{\mathfrak{p}}^2$. Hence there exists a unique element $\mathfrak{d}(\mathfrak{A})$ of $J_{\mathsf{K}}/U_{\mathsf{K}}^2$ whose $\mathfrak{p}$-components are the $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{A})$. The ideal $(\mathfrak{d}(\mathfrak{A}))$ coincides with the discriminant of $\mathfrak{A}$ defined by ARTIN (cf. [1]). Here we have — as in [4] — considered $J_{\mathsf{K}}/U_{\mathsf{K}}^2$ as the subgroup of the cartesian product $\prod_{\mathfrak{p}} \mathsf{K}_{\mathfrak{p}}^{\times}/U_{\mathfrak{p}}^2$ whose elements have their $\mathfrak{p}$-components in $U_{\mathfrak{p}}/U_{\mathfrak{p}}^2$ almost everywhere.

We first note

2.1. $\mathfrak{d}(\mathfrak{A}) \in J_{\mathsf{K}}^2 P_{\mathsf{K}}/U_{\mathsf{K}}^2$ *and* $\mathfrak{d}(\mathfrak{A})\,\mathfrak{d}(\Lambda/\mathsf{K})^{-1} \in J_{\mathsf{K}}^2/U_{\mathsf{K}}^2$.

PROOF. By [4] (cf. 2.2) it will suffice to establish the second relation in 2.1. For each $\mathfrak{p}$, an $\mathfrak{o}_{\mathfrak{p}}$-basis of $\mathfrak{A}_{\mathfrak{p}}$ is at the same time a $\mathsf{K}_{\mathfrak{p}}$-basis of $\Lambda_{\mathfrak{p}}$. The discriminant of such a basis is determined by $\Lambda_{\mathfrak{p}}$ modulo $\mathsf{K}_{\mathfrak{p}}^{\times 2}$. Hence if $\mathfrak{B}$ is another ideal in K, $\mathfrak{d}_{\mathfrak{p}}(\mathfrak{A})\,\mathfrak{d}_{\mathfrak{p}}(\mathfrak{B})^{-1} \in \mathsf{K}_{\mathfrak{p}}^{\times 2}/U_{\mathfrak{p}}^2$, and so $\mathfrak{d}(\mathfrak{A})\,\mathfrak{d}(\mathfrak{B})^{-1} \in J_{\mathsf{K}}^2/U_{\mathsf{K}}^2$. This is in particular the case for $\mathfrak{B} = \mathfrak{O}$.

The endomorphism $\mathfrak{m} \to \mathfrak{m}^2$ of the idèle group gives rise to homomorphisms

$$\tau: J_K/U_K \to J_K^2/U_K^2 \tag{2.1}$$

and

$$\sigma: J_K/P_K U_K \to J_K^2/P_K^2 U_K^2. \tag{2.2}$$

It is easily seen that σ and τ are isomorphisms.

As $J_K^2 \cap P_K U_K^2 = P_K^2 U_K^2$ we obtain a direct product representation

$$J_K^2 P_K/U_K^2 P_K^2 \cong J_K^2/U_K^2 P_K^2 \times U_K^2 P_K/U_K^2 P_K^2 \tag{2.3}$$

with associated epimorphisms

$$J_K^2 P_K/U_K^2 P_K^2 \to J_K^2/U_K^2 P_K^2,$$
$$J_K^2 P_K/U_K^2 P_K^2 \to U_K^2 P_K/U_K^2 P_K^2.$$

Composing each of these mappings with the epimorphism

$$J_K^2 P_K/U_K^2 \to J_K^2 P_K/U_K^2 P_K^2$$

we obtain epimorphisms

$$\lambda: J_K^2 P_K/U_K^2 \to J_K^2/U_K^2 P_K^2, \tag{2.4}$$

$$\mu: J_K^2 P_K/U_K^2 \to U_K^2 P_K/U_K^2 P_K^2. \tag{2.5}$$

By 2.1 $\mathfrak{d}(\mathfrak{A})\,\mathfrak{d}(\Lambda/K)^{-1}$ will fall into the first component of the decomposition (2.3) and so

2.2. $\mu(\mathfrak{d}(\mathfrak{A})) = \mu(\mathfrak{d}(\Lambda/K))$ *solely depends on* Λ.

To evaluate $\mu(\mathfrak{d}(\Lambda/K))$ we have only to choose some element $\delta \in K^\times$ which is the discriminant of a K-basis of Λ. As shown in [4] (cf. 2.2) the representatives of $\mathfrak{d}(\Lambda/K)$ in J_K are then of form $\delta\mathfrak{m}^2$. Thus $\mu(\mathfrak{d}(\Lambda/K))$ is the class of δ mod $U_K^2 P_K^2$. At the same time we see that

$$\lambda(\mathfrak{d}(\mathfrak{A})) = [\delta^{-1} U_K^2 \cdot \mathfrak{d}(\mathfrak{A})] \cdot P_K^2. \tag{2.6}$$

We can now determine the module invariant $C(\mathfrak{A})$ in terms of $\mathfrak{d}(\mathfrak{A})$.

2.3. Theorem. $C(\mathfrak{A}) = \sigma^{-1}\lambda(\mathfrak{d}(\mathfrak{A}))$.

Theorem 2.5 in [4], which gave a necessary and sufficient criterion for the existence of a free $\mathfrak{o}$-basis of $\mathfrak{O}$, is a special case of 2.3. We have in fact by 2.3.

2.4. $\mathfrak{A}$ *has a free* $\mathfrak{o}$*-basis if, and only if* $\mathfrak{d}(\mathfrak{A}) \in U_K^2 P_K/U_K^2$.

The determination of $C(\mathfrak{A})$ by means of $\mathfrak{d}(\mathfrak{A})$ can of course also be expressed in purely ideal theoretic form. We consider the ideal $(\mathfrak{d}(\mathfrak{A}))$, i.e. the class of $\mathfrak{d}(\mathfrak{A})$ mod U_K; if $\mathfrak{A} = \mathfrak{O}$ this is the classical relative discriminant. By 2.1 the absloute ideal class of $(\mathfrak{d}(\mathfrak{A}))$ is the square of a class C_1. This of course will not yet determine C_1 uniquely; each such class contains ideals $\mathfrak{b}$ such that $\mathfrak{b}^2(\alpha) = (\mathfrak{d}(\mathfrak{A}))$ for some $\alpha \in K^\times$. We obtain $C(\mathfrak{A})$ by taking α as the

discriminant of some K-basis of Λ. $(\mathfrak{d}(\mathfrak{A}))\,(\alpha)^{-1}$ will then be the square of an ideal $\mathfrak{b}$, whose class is $C(\mathfrak{A})$. In this ideal theoretic form ARTIN derived his criterion for the existence of a free $\mathfrak{o}$-basis of $\mathfrak{O}$ (cf. [1]).

PROOF OF 2.3. Let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ be a K-basis of Λ with discriminant α and let $\mathfrak{B}$ be the free $\mathfrak{o}$-module generated by this basis. Then

$$C(\mathfrak{A}) = [\mathfrak{B}:\mathfrak{A}] \cdot U_{\mathsf{K}} P_{\mathsf{K}},$$

and so

$$\sigma\big(C(\mathfrak{A})\big) = \tau([\mathfrak{B}:\mathfrak{A}]) \cdot U_{\mathsf{K}}^2 P_{\mathsf{K}}^2. \tag{2.7}$$

Let $\mathfrak{m}$ be a representative of $\mathfrak{d}(\mathfrak{A})$ in J_{K}. For each prime divisor $\mathfrak{p}$ there exists an $\mathfrak{o}_{\mathfrak{p}}$-basis $\beta^{(1)}, \ldots, \beta^{(n)}$ of $\mathfrak{A}_{\mathfrak{p}}$ with discriminant $\mathfrak{m}_{\mathfrak{p}}$. Moreover there will exist a non singular matrix $A_{\mathfrak{p}} = (a_{ij})$ with elements in $\mathsf{K}_{\mathfrak{p}}$ such that

$$\beta^{(i)} = \sum_{j=1}^{n} a_{ij} \alpha_{\mathfrak{p}}^{(j)} \qquad (i = 1, \ldots, n).$$

Hence

$$\mathfrak{m}_{\mathfrak{p}} = |A_{\mathfrak{p}}|^2 \alpha_{\mathfrak{p}}. \tag{2.8}$$

The idèle $\mathfrak{n}$ with $\mathfrak{p}$-components $|A_{\mathfrak{p}}|$ is then a representative in J_{K} of $[\mathfrak{B}:\mathfrak{A}]$. Hence $\mathfrak{n}^2$ is a representative of $\tau([\mathfrak{B}:\mathfrak{A}])$, and so

$$\tau([\mathfrak{B}:\mathfrak{A}]) = \mathfrak{n}^2 U_{\mathsf{K}}^2. \tag{2.9}$$

But we have by (2.8) $\mathfrak{m} = \mathfrak{n}^2 \alpha$ and so $\mathfrak{d}(\mathfrak{A}) = \mathfrak{n}^2 U_{\mathsf{K}}^2 \cdot \alpha\, U_{\mathsf{K}}^2$. Therefore

$$\lambda\big(\mathfrak{d}(\mathfrak{A})\big) = \mathfrak{n}^2 U_{\mathsf{K}}^2 P_{\mathsf{K}}^2. \tag{2.10}$$

By (2.7), (2.9) and (2.10) the theorem now follows.

2.5. THEOREM.

$$\mathfrak{d}(\mathfrak{A}) = \mathfrak{d}(\Lambda/\mathsf{K}) \cdot \tau(N_{\Lambda/\mathsf{K}}\mathfrak{A}).$$

This theorem is seen to determine $\mathfrak{d}(\mathfrak{A})$ in terms of the ideal $N_{\Lambda/\mathsf{K}}\mathfrak{A}$. As τ is an isomorphism it also determines $N_{\Lambda/\mathsf{K}}\mathfrak{A}$ in terms of $\mathfrak{d}(\mathfrak{A})$ in analogy to the classical formula for absolute norms. 2.5 — in ideal theoretic form — is due to ARTIN (cf. [1]).

PROOF OF 2.5. Let $\mathfrak{m}$, $\mathfrak{n}$ be representatives in J_{K} of $\mathfrak{d}(\mathfrak{A})$ and of $\mathfrak{d}(\mathfrak{O})$ respectively. For each prime divisor $\mathfrak{p}$ there exists a basis $\alpha^{(1)}, \ldots, \alpha^{(n)}$ of $\mathfrak{A}_{\mathfrak{p}}$ with discriminant $\mathfrak{m}_{\mathfrak{p}}$ and a basis $\beta^{(1)}, \ldots, \beta^{(n)}$ of $\mathfrak{O}_{\mathfrak{p}}$ with discriminant $\mathfrak{n}_{\mathfrak{p}}$. Moreover we obtain a non singular matrix $A_{\mathfrak{p}} = (a_{ij})$ with elements in $\mathsf{K}_{\mathfrak{p}}$ such that

$$\alpha^{(i)} = \sum_{j=1}^{n} a_{ij} \beta^{(j)} \qquad (i = 1, \ldots, n),$$

so that we get

$$\mathfrak{m}_{\mathfrak{p}} = |A_{\mathfrak{p}}|^2 \mathfrak{n}_{\mathfrak{p}}.$$

Let $\mathfrak{r}$ be the idèle with $\mathfrak{p}$-components $|A_\mathfrak{p}|$. Then

$$\mathfrak{m} = \mathfrak{r}^2 \mathfrak{n}. \tag{2.11}$$

On the other hand $\mathfrak{r}_\mathfrak{p}$ generates the local ideal $N_{\Lambda_\mathfrak{p}/\mathsf{K}_\mathfrak{p}} \mathfrak{A}_\mathfrak{p}$ and so $\mathfrak{r} U_\mathsf{K} = N_{\Lambda/\mathsf{K}} \mathfrak{A}$. Hence

$$\mathfrak{r}^2 U_\mathsf{K}^2 = \tau(N_{\Lambda/\mathsf{K}} \mathfrak{A}).$$

Comparison with (2.11) gives the theorem.

As the norm is multiplicative we get by 2.5.

2.6. $\mathfrak{d}(\mathfrak{A}\mathfrak{B})\,\mathfrak{d}(\Lambda/\mathsf{K}) = \mathfrak{d}(\mathfrak{A})\,\mathfrak{d}(\mathfrak{B})$.

From this equation and from 2.3 we have

2.7. Theorem.

$$C(\mathfrak{A}\mathfrak{B})\,C(\mathfrak{D}) = C(\mathfrak{A})\,C(\mathfrak{B}).$$

Next we derive a relation between the module invariant $C(\mathfrak{A})$ and the relative norm $N_{\Lambda/\mathsf{K}}\mathfrak{A}$. Recall that $C(N_{\Lambda/\mathsf{K}}\mathfrak{A})$ is the absolute ideal class of $N_{\Lambda/\mathsf{K}}\mathfrak{A}$.

2.8. Theorem [2]).

$$C(\mathfrak{A}) = C(\mathfrak{D})\,C(N_{\Lambda/\mathsf{K}}\mathfrak{A}).$$

Proof. By 2.3, 2.5,

$$\sigma\big(C(\mathfrak{A})\big) = \sigma\big(C(\mathfrak{D})\big)\,\lambda\,\tau(N_{\Lambda/\mathsf{K}}\mathfrak{A}).$$

As $\tau(N_{\Lambda/\mathsf{K}}\mathfrak{A})$ lies in $J_\mathsf{K}^2/U_\mathsf{K}^2$ we see that $\lambda\tau(N_{\Lambda/\mathsf{K}}\mathfrak{A})$ is simply the class of $\tau(N_{\Lambda/\mathsf{K}}\mathfrak{A})$ modulo $U_\mathsf{K}^2 P_\mathsf{K}^2$, and so coincides with $\sigma\big(C(N_{\Lambda/\mathsf{K}}\mathfrak{A})\big)$.

We note a number of Corollaries of 2.8.

2.9. *If $\mathfrak{D}$ has a free $\mathfrak{o}$-basis then*

$$C(\mathfrak{A}) = C(N_{\Lambda/\mathsf{K}}\mathfrak{A}).$$

2.10. *A necessary and sufficient condition for the existence of an ideal $\mathfrak{A}$ in Λ which has a free $\mathfrak{o}$-basis is that the ideal class $C(\mathfrak{D})$ should contain an ideal norm of Λ.*

Finally we note that the classes $C(\mathfrak{A})$ will by 2.8 lie in a fixed coset of the absolute class group modulo the subgroup of classes containing ideal norms. We thus obtain an interesting relation between the $\mathfrak{o}$-module types possible in Λ and the intersection of Λ with the absolute class field of K.

2.11. Theorem. *Let $\overline{\mathsf{K}}$ be the absolute class field of K and h_K the absolute class number. The number of non $\mathfrak{o}$-isomorphic ideals in a finite extension Λ of K is then $h_\mathsf{K}/(\Lambda\cap\overline{\mathsf{K}}:\mathsf{K})$. In particular all $\mathfrak{o}$-isomorphism classes of $\mathfrak{o}$-modules of rank $(\Lambda:\mathsf{K})$ are represented by ideals in Λ, if and only if $\Lambda\cap\overline{\mathsf{K}}=\mathsf{K}$. All ideals in Λ are $\mathfrak{o}$-isomorphic if and only if $\Lambda \supseteq \overline{\mathsf{K}}$.*

[2]) This theorem is closely related to Theorem 10 in [2].

2.11 leads to a module theoretic characterisation of $\overline{K}$:

2.12. *The absolute class field* $\overline{K}$ *of* K *is the unique minimal extension of* K *with the property that all ideals are* $\mathfrak{o}$*-isomorphic.*

References

[1] ARTIN, E.: Questions de la base minimale dans la théorie des nombres algébriques. Centre Nat. Rech. Sci. XXIV (Colloq. Int., Paris, 1949), 19—20. — [2] CHEVALLEY, C.: L'Arithmétique dans les Algèbres de Matrices. Actualités scient. et. industr. 323 (1936). — [3] FRANZ, W.: Elementarteilertheorie in algebraischen Zahlkörpern. J. reine angew. Math. **171**, 149—161 (1934). — [4] FRÖHLICH, A.: Discriminants of algebraic number fields. Math. Z. **74**, 18—28 (1960). — [5] KAPLANSKY, I.: Modules over Dedekind Rings and Valuation Rings. Trans. Amer. Math. Soc. **72**, 327—340 (1952). — [6] KRULL, W.: Matrizen, Moduln und verallgemeinerte Abelsche Gruppen im Bereich der ganzen algebraischen Zahlen. Sitzungsber. Heidelberg. Akad. Wiss., Math.-nat. Kl. **1932**, 13—38. — [7] SCHUR, I.: Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlenkörper. Math. Ann. **71**, 354—367 (1911). — [8] STEINITZ, E.: Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. I, II. Math. Ann. **71**, 328—353; **72**, 297—345 (1911).

King's College, London W.C. 2 (England)

(Eingegangen am 15. September 1959)

Menzel, W.
Math. Zeitschr. 74, 39—51 (1960)

Über den Untergruppenverband einer Abelschen Operatorgruppe Teil I: m-Verbände

Von

Wolfram Menzel

Einleitung

Die endlichen distributiven Verbände lassen sich bekanntlich kennzeichnen als die Teilverbände der Potenzmengen geeigneter endlicher Mengen (vgl. Hermes [7], § 20). Raney [8], Balachandran [2], Bruns [5] gaben verbandstheoretische Charakterisierungen solcher Verbände, welche verbandsisomorph einem vollständigen Teilverbande der Potenzmenge einer (beliebigen) Menge sind. So lautet der Darstellungssatz von Raney und Balachandran: *Genau dann ist der vollständige Verband L einem vollständigen Teilverbande einer Potenzmenge isomorph, wenn jedes Element von L Verbindung perfekter Elemente ist.* (Wie in 1.3 heiße ein Element $p \in L$ *perfekt*, wenn für jede Teilmenge X von L aus $p < \bigvee_{x \in X} x$ folgt $p < x$ für ein $x \in X$.) Auch die vorliegende Arbeit behandelt Verbände mit dieser Eigenschaft; wir nennen sie m-Verbände.

Bekanntlich läßt sich aus der Gültigkeit — auch beliebig allgemeiner — Distributivitätsgesetze allein noch nicht die m-Eigenschaft folgern (vgl. Raney [8], S. 680). Um diese zu erhalten, hat man vielmehr auch die Endlichkeit des Verbandes in geeigneter Weise zu verallgemeinern: Nennt man ein Element eines Verbandes *voll $\cup$-irreduzibel*, wenn es nicht als Verbindung echt früherer dargestellt werden kann, so sei jedes Verbandselement Verbindung von voll $\cup$-irreduziblen Elementen. Verbände mit dieser Eigenschaft bezeichnen wir als *glatt*. Es ergibt sich nun (als Verallgemeinerung des eingangs erwähnten Satzes über endliche distributive Verbände): Ein vollständiger Verband ist genau dann m-Verband, wenn er glatt ist und dem einen unendlich-distributiven Gesetz (D^*1) (s. 1.1) genügt (Satz 1, 3.6). Bis auf Verbandsisomorphie ist er dann völlig charakterisiert durch die Halbordnung seiner voll $\cup$-irreduziblen Elemente. Umgekehrt gibt es zu beliebig vorgegebener Halbordnung H stets einen und (bis auf Verbandsisomorphie) nur einen m-Verband, dessen voll $\cup$-irreduzible Elemente eine Halbordnung isomorph zu H bilden. Es besteht so eine eineindeutige reziproke Beziehung zwischen den Klassen verbandsisomorpher m-Verbände und halbordnungsisomorpher Halbordnungen (Satz 2, 3.7). Diese bewirkt, daß sich Kettenbedingungen für die Halbordnung in solchen für den Verband spiegeln (Satz 3, 5.2).

§ 1. Voll ∪-irreduzible und perfekte Elemente eines Verbandes

1.1. In einer Halbordnung H mit Elementen $x, y, \ldots$ bezeichnen wir in der üblichen Weise die Halbordnungsrelation mit „$\subset$" („früher"). Für $y \subset x$, $y \neq x$ schreiben wir $y \subset' x$. Ist ferner y „unterer Nachbar" von x ($y \subset' x$, und $y \subset' z \subset x$ impliziert $z = x$), so werde dies durch „$y \prec x$" kenntlich gemacht.

Zur Unterscheidung von der „allgemeinen" Halbordnungsrelation „$\subset$" drücken wir das (mengentheoretische) Enthaltensein einer Menge Y in einer anderen X durch $Y \subset_m X$ aus. Echtes Enthaltensein ist durch $\subset'_m$ gekennzeichnet.

Sei A ein Verband. Wie üblich bezeichnen wir die Verbandsoperationen mit $\cap$ und $\cup$. Jeder vollständige Verband besitzt ein „Nullelement" 0 und ein „Eins- (All-) Element", das wir mit 1 bezeichnen wollen.

Wir gebrauchen zur Abkürzung die folgende Komplexschreibweise für Schnitte und Verbindungen in einem vollständigen Verbande A: Ist X eine Teilmenge von A, y ein Element von A so sei,

$$\wedge X = \bigwedge_{x \in X} x, \qquad X \cap y = \{x \cap y;\ x \in X\}$$

und entsprechend für Verbindungen; ist ferner $\mathfrak{X}$ eine Menge von Teilmengen von A, so sei

$$\wedge\wedge \mathfrak{X} = \bigwedge_{X \in \mathfrak{X}} (\wedge X), \quad \text{analog } \wedge\vee\mathfrak{X}, \quad \vee\wedge\mathfrak{X}, \quad \vee\vee\mathfrak{X}.$$

Bezeichnet man zu einer Menge $\mathfrak{X}$ von Mengen mit $\Phi(\mathfrak{X})$ die Menge aller Funktionen auf $\mathfrak{X}$, die jedem $X \in \mathfrak{X}$ ein Element $x \in X$ zuordnen, bezeichnet man ferner durch $\check{\varphi}$ den Wertevorrat einer Funktion $\varphi \in \Phi(\mathfrak{X})$, so sei $\check{\mathfrak{X}} = \{\check{\varphi};\ \varphi \in \Phi(\mathfrak{X})\}$.

Entsprechend der Bezeichnung $\subset_m$ für mengentheoretisches Enthaltensein drücken wir mengentheoretische Durchschnitts- bzw. Vereinigungsbildung durch $\cap_m$, $\cup_m$ aus. Das Zeichen für die mengentheoretische Differenz sei $\dot{-}$. Ist m eine Menge, so wollen wir die „Potenzmenge" von m — die Menge aller Teilmengen der Menge m — stets $\mathfrak{P}(m)$ nennen.

Die Halbordnungsrelation in einem Verbande induziert eine Halbordnungsrelation in jeder seiner Teilmengen. Eine Teilmenge eines Verbandes A heißt *Unterverband von* A, wenn sie bezüglich der in ihr induzierten Halbordnungsrelation einen Verband bildet. Der Unterverband B des vollständigen Verbandes A heißt *vollständiger Teilverband* von A, wenn B ein vollständiger Verband ist, und der in B gebildete Schnitt bzw. die in B gebildete Verbindung einer Menge von Elementen aus B gleich ihrem in A gebildeten Schnitt bzw. ihrer in A gebildeten Verbindung ist. Der Unterverband B von A ist genau dann vollständiger Teilverband von A, wenn für beliebiges $X \subset_m B$ der in A gebildete Schnitt $\wedge X$ und die in A gebildete Verbindung $\vee X$ in B liegen (vgl. HERMES [7], § 6). Bekanntlich nennt man einen Verband A *distributiv*, wenn er das Gesetz

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$$

für beliebige $x, y, z \in A$ erfüllt. Darüber hinaus gibt es die Gesetze „beliebiger" Distributivität:

Der vollständige Verband A heiße (D^* 1)- bzw. (D^* 2)-*Verband*, wenn für Elemente $a \in A$ und Teilmengen B von A stets gilt

$$(D^*\,1) \quad a \cap \bigvee B = \bigvee (a \cap B)$$

bzw.

$$(D^*\,2) \quad a \cup \bigwedge B = \bigwedge (a \cup B).$$

Erfüllt A für beliebige Mengen $\mathfrak{A} \subset_m \mathfrak{P}(A)$ von Teilmengen X von A uneingeschränkt die Gesetze

$$\bigwedge \bigvee \mathfrak{A} = \bigvee \bigwedge \breve{\mathfrak{A}}$$

$$\bigvee \bigwedge \mathfrak{A} = \bigwedge \bigvee \breve{\mathfrak{A}},$$

so heißt A *voll distributiv*.

Der Verband $\mathfrak{P}(m)$ aller Teilmengen einer Menge m ist voll distributiv, und ebenso ist es jeder vollständige Teilverband von $\mathfrak{P}(m)$ (s. Hermes [7], S. 132, 133).

Ein endlicher distributiver Verband ist durch die Halbordnung der in ihm „irreduziblen" Elemente bestimmt (Birkhoff [3], IX, § 4). Wir definieren demgemäß für Verbände ohne Endlichkeitsbedingungen:

1.2. Definition. Ein Element i des Verbandes A heißt *voll $\cup$-irreduzibel* (v. i.) *in* A, wenn für jede Menge $X \subset_m A$ gilt: Aus $i = \bigvee X$ folgt $i \in X$.

Die voll $\cup$-irreduziblen Elemente von A bilden eine Halbordnung $H \subset_m A$.

(Bekanntlich heißt ein Element j $\cup$-irreduzibel, wenn aus $j = x \cup y$ folgt $j = x$ oder $j = y$).

Daß nicht jedes $\cup$-irreduzible Element auch v. i. ist, zeigt folgendes Beispiel:

A sei die Menge der Zahlen 0, 1, 2, 3, ... mit der Definition: Es sei dann und nur dann $b < a$, wenn es ein $q \in A$ mit $a = bq$ gibt. Dann ist 0 das Allelement in A und $0 = \bigvee_{k=1}^{\infty} k$ nicht v. i. 0 ist irreduzibel, denn aus

$$0 = x \cup y = \text{k.g.V.}[x, y] \quad \text{folgt} \quad 0 = x \quad \text{oder} \quad 0 = y.$$

Ist A distributiv und i ein irreduzibles Element in A, so folgt für jede *endliche* Teilmenge X von A:

Wenn $i < \bigvee X$, so $i < x$ für ein $x \in X$. Dies legt die folgende Definition nahe, welche in engem Zusammenhange mit der Einbettbarkeit eines Verbandes in eine Potenzmenge steht:

1.3. Definition. Ein Element $p \in A$ heißt *perfekt*, wenn für alle $X \subset_m A$ aus $p < \bigvee X$ folgt, daß $p < x$ für ein $x \in X$ gilt.

Es ist klar, daß jedes perfekte Element v. i. ist.

1.4. *In einem (D^* 1)-Verbande bedeuten Perfektheit und volle Irreduzibilität dasselbe.*

Beweis. Sei i ein Element der Halbordnung H aller v. i. Elemente von A; sei ferner $i < \bigvee X$ für ein $X \subset_m A$. Dann gilt: Aus $i < \bigvee X$ folgt $i = i \cap \bigvee X$,

und weiter $i = \vee(i \cap X)$ nach (D^*1), $i \in i \cap X$ wegen $i \in H$, also $i < x$ für ein $x \in X$.

Insbesondere bedeuten in einem vollständigen Teilverbande einer Potenzmenge Perfektheit und volle Irreduzibilität dasselbe.

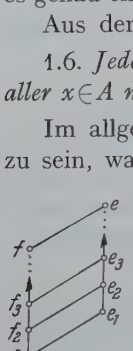
Wir sagen entsprechend dem von WIELANDT in [9] für Gruppen eingeführten Ausdruck

1.5. DEFINITION. Ein Element eines Verbandes A heißt *einköpfig*, wenn es genau einen unteren Nachbar besitzt.

Aus der Definition der vollen Irreduzibilität folgt dann sofort

1.6. *Jedes $i \in H$ ist einköpfig mit dem unteren Nachbarn i', der Verbindung aller $x \in A$ mit $x < 'i$.*

Im allgemeinen braucht nicht jedes einköpfige Element voll irreduzibel zu sein, was etwa an einem Verbande der folgenden Gestalt deutlich wird



(Die e_i, $i = 1, 2, \ldots$ bilden eine unendliche aufsteigende Kette mit der Verbindung e; f ist einziger unterer Nachbar von e.)

Jedoch gilt:

1.7. *In einem $\downarrow$-atomaren Verbande ist jedes einköpfige Element v. i.*

Dabei heißt nach BIRKHOFF [1], S. 38, ein Verband A $\uparrow$- bzw. $\downarrow$-atomar, wenn sich je zwei Elemente $a, b \in A$ mit $b < 'a$ durch eine maximale, aufsteigend bzw. absteigend wohlgeordnete Kette verbinden lassen. Es ist klar, daß $\downarrow$-Atomarität äquivalent der Eigenschaft ist: „Zu $a, b \in A$ mit $b < 'a$ gibt es stets untere Nachbarn von a über b", und eine entsprechende Aussage gilt für $\uparrow$-Atomarität. Für die genannten Eigenschaften eines Verbandes sind auch die Bezeichnungen „schwache Minimalbedingung" bzw. „schwache Maximalbedingung" üblich.

BEWEIS zu 1.7. Sei e einköpfig mit dem einzigen unteren Nachbarn $f < e$. Wäre $e \notin H$, so müßte es ein $u \in A$ geben mit $u < 'e$, $u \not\subset f$. Aus der $\downarrow$-Atomarität folgt die Existenz eines $v \in A$ mit $u < v < e$. Man hätte $v \not\subset f$, also einen zweiten unteren Nachbarn von e.

§ 2. Bänder in einer Halbordnung

Sei jetzt H eine beliebige Halbordnung.

2.1. DEFINITION. Eine Teilmenge B von H ist ein *Band in H*, wenn für beliebige $x \in B$ und $y \in H$ gilt: Aus $y < x$ folgt $y \in B$.

2.2. *Die Menge $\mathfrak{B}(H)$ der Bänder einer Halbordnung H ist ein vollständiger Verband bei mengentheoretischer Schnitt- und Verbindungsbildung, somit vollständiger Teilverband der Potenzmenge $\mathfrak{P}(H)$.*

2.3. *Die in $\mathfrak{B}(H)$ voll irreduziblen Elemente sind die „Hauptbänder" $\tilde{i} = \{k; k \in H, k < i$ für (festes) $i \in H\}$. Sie bilden eine Halbordnung isomorph zu H.*

BEWEIS zu 2.2. Zu zeigen ist, daß für jede Menge $\mathfrak{C} <_m \mathfrak{B}$ von Bändern die Mengen $\bigwedge_{C \in \mathfrak{C}}{}_m C$, $\bigvee_{C \in \mathfrak{C}}{}_m C$ Bänder sind. In der Tat gilt für beliebiges $y \in H$

Aus $x \in \bigwedge_{C \in \mathfrak{C}}{}_m C$ und $y < x$ folgt $x \in C$ für alle $C \in \mathfrak{C}$ und $y < x$, also $y \in C$ für alle $C \in \mathfrak{C}$ (da $\mathfrak{C} <_m \mathfrak{B}$); also $y \in \bigwedge_{C \in \mathfrak{C}}{}_m C$.

Aus $x \in \bigvee_{C \in \mathfrak{C}}{}_m C$ und $y < x$ folgt die Existenz eines $C_0 \in \mathfrak{C}$ mit $x \in C_0$, also $y < C_0$ (da $C_0 \in \mathfrak{B}$), also $y \in \bigvee_{C \in \mathfrak{C}} C$.

Beweis zu 2.3. Jedes „Hauptband" ist voll irreduzibel, denn ist $\tilde{i}$ eine Vereinigung von Bändern, $\tilde{i} = \bigvee_m X$, $(X \in \mathfrak{X} <_m \mathfrak{B})$, so $i \in X$ für ein $X \in \mathfrak{X}$, also $\tilde{i} <_m X$, da X Band, mithin $\tilde{i} = X$. Ist umgekehrt B nicht Hauptband, so gilt $\tilde{i} <'_m B$ für alle $i \in B$. Da aber andererseits $B = \bigvee_{i \in B}{}_m i$ ist, folgt: B ist nicht v. i. in $\mathfrak{B}$.

Die Äquivalenz von $k < i$ und $\tilde{k} <_m \tilde{i}$ ist klar: Die Hauptbänder bilden eine Halbordnung isomorph zu H.

§ 3. Glatte Verbände, m-Verbände

3.1. Sei A ein Verband, H die Halbordnung der v. i. Elemente in A. Jedem $a \in A$ läßt sich in eindeutiger Weise die Menge

$$\tilde{a} = \{i;\ i \in H,\ i < a\}$$

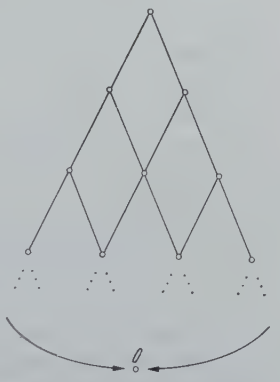
zuordnen.

Man sieht sofort, daß $\tilde{a}$ ein Band in H ist.

3.2. Definition. Der Verband A heißt *glatt*, wenn er vollständig ist und jedes seiner Elemente Verbindung voll irreduzibler ist.

Es ist klar, daß A genau dann glatt ist, wenn für alle $a \in A$ gilt $\bigvee \tilde{a} = a$.

Beispiel für einen nicht leeren vollständigen Verband ohne v. i. Elemente — einen Verband also, der sicherlich nicht glatt ist — ist etwa der in nebenstehendem Schema dargestellte Verband.



(Es ist klar, wie der Verband, vom Allelement ausgehend, zu konstruieren ist. Er werde in der durch Punkte angedeuteten Weise nach „unten" unendlich weit fortgesetzt und schließlich 0 als Schnitt aller Verbandselemente dazu erklärt.) Der Verband ist sogar distributiv.

3.3. *Jeder vollständige Verband A mit Minimalbedingung ist glatt.*

Beweis. A sei nicht glatt, die Menge $N <_m A$ der nicht als Verbindung von v. i. Elementen darstellbaren Elemente aus A also nicht leer. Gäbe es ein minimales Element n in N, so wäre dieses jedenfalls nicht v. i. Also gälte (für eine Teilmenge X von A)

$$n = \bigvee X, \quad x <' n \quad \text{für alle} \quad x \in X.$$

Aus der Minimalität von n aber folgte dann

$$x = \vee Y_x, \quad Y_x \subset_m H \quad \text{für alle} \quad x \in X,$$

und hieraus die Darstellbarkeit von $n = \vee X$.

Wir hätten somit $n \notin N$ entgegen der Annahme.

N kann also kein minimales Element enthalten, und dies widerspricht wegen $N \neq \emptyset$ der Minimalbedingung.

In den weiteren Untersuchungen werden vornehmlich Verbände eine Rolle spielen, die verbandsisomorph einem vollständigen Teilverband einer Potenzmenge $\mathfrak{P}(m)$ sind. Da die (für solch einen Verband naheliegende) Bezeichnung „Mengenverband" in anderem Sinne verwandt wird (HERMES [7], S. 54), ein an „Menge" erinnernder Name aber zu wünschen ist, sagen wir:

3.4. DEFINITION. Ein Verband heißt m-*Verband*, wenn er verbandsisomorph einem vollständigen Teilverband einer Potenzmenge $\mathfrak{P}(m)$ ist.

3.5. *Mit A ist auch jeder vollständige Teilverband B von A ein* m-*Verband.*

(Das folgt sofort aus 3.4 und der Definition eines vollständigen Teilverbandes B von A: B ist einem vollständigen Teilverbande derselben Potenzmenge wie A verbandsisomorph.) Insbesondere wird jedes „Intervall" $[b, a] = \{x;\ x \in A,\ b < x < a\}$, wo a, b beliebige Elemente von A sind, ein m-Verband.

Es gilt nun

3.6. SATZ 1. *Für einen vollständigen Verband A sind äquivalent*

(1) *A ist* m-*Verband.*

(2) *A ist glatter $(D^*\ 1)$-Verband.*

(3) *Jedes Element von A ist Verbindung perfekter Elemente.*

BEWEIS. Die Äquivalenz von (1) und (3) ist der Inhalt von RANEY [8], Theorem 2.

Wegen 1.4 folgt (3) aus (2).

Gelte (1); die volle Distributivität einer Potenzmenge impliziert, daß auch jeder ihrer vollständigen Teilverbände, somit jeder m-Verband volldistributiv ist. Erst recht genügt ein solcher $(D^*\ 1)$, und da jedes perfekte Element v. i. ist, folgt (2) [1]).

Von BRUNS [5] wurde noch gezeigt: A ist genau dann m-Verband wenn $(D^*\ 1)$ und $(D^*\ 2)$ gelten und zudem jedes Intervall in A einen Sprung enthält. (Ein Sprung $\langle b, a \rangle$ ist ein Intervall $[b, a]$ mit $b \prec a$.) BRUNS selbst hat in der genannten Arbeit die Verbindung zwischen diesen Eigenschaften einerseits und der Darstellung der Verbandselemente durch v. i. andererseits hergestellt (S. 111). Die von ihm beim Beweis des genannten Satzes verwendete Zuordnung φ

$$a \xrightarrow{\varphi} \{\langle x, y \rangle;\ x \cup a > y\}$$

[1]) Es mag wünschenswert scheinen, die Äquivalenz von (1) und (2) unabhängig von RANEY's Ergebnis zu beweisen. Jedoch führt dies (wie durch 1.4 auch nahegelegt ist) doch wiederum auf den Beweis, den bereits RANEY verwendet hat. Zudem wird die Implikation „Aus (2) folgt (1)" nochmals im Beweis von Satz 2 [Teil (α)] mitbewiesen.

von Mengen von Sprüngen zu Verbandselementen entspricht der Zuordnung $a \to \tilde{a}$ in folgendem Sinne: In einem m-Verbande gibt es zu jedem Sprung $\langle x, y \rangle$ genau ein $i \in H$ mit $x \cdot i = y$ (s. 5.5). Es ist dann $y \cdot x \cdot a$ äquivalent mit $i \subset a$.

3.7. Satz 2. *Ein* m-*Verband* A *ist vollständig charakterisiert durch die Halbordnung* H *der in ihm v. i. Elemente: nämlich isomorph dem Verbande der Bänder in* H.

Umgekehrt gibt es zu jeder vorgegebenen Halbordnung H *einen und bis auf Isomorphie nur einen* m-*Verband, dessen v. i. Elemente eine Halbordnung isomorph zu* H *bilden.*

Es besteht so eine reziproke Beziehung zwischen den Klassen halbordnungsisomorpher Halbordnungen und verbandsisomorpher m-*Verbände.*

Beweis. (α) H sei die Halbordnung der v. i. Elemente des m-Verbandes A. Wir betrachten die Abbildung $a \xrightarrow{\beta} \beta(a) = \tilde{a}$ von A in den Bänderverband $\mathfrak{B} = \mathfrak{B}(H)$ und zeigen, daß β ein Verbandsisomorphismus ist.

$\tilde{a} \in \mathfrak{B}$ und die Eindeutigkeit der Abbildung wurde bereits festgestellt. β ist Abbildung *auf* $\mathfrak{B}$. Denn für $i \in H$ gilt, wenn B ein Band in H ist, $i \subset \vee B$ genau dann, wenn $i \subset k$ für ein $k \in B$ ist (da i perfekt), also wenn $i \in B$ ist. Es folgt $\beta(\vee B) = \widetilde{\vee B} = B$.

Wegen der Glätte von A ist für $a \in A$ stets $\vee \tilde{a} = a$, und es folgt, daß die Abbildung β und die durch $\mathfrak{B} \ni B \to \vee B \in A$ definierte Abbildung β^* eine reziproke (also eineindeutige) Beziehung zwischen A und $\mathfrak{B}$ bewirken: $\beta^* = \beta^{-1}$.

Weiter gilt für β, wenn X eine beliebige Teilmenge von A ist,

$$\beta(\wedge X) = \wedge_m \tilde{x} \quad (x \in X)$$

$$\beta(\vee X) = \vee_m \tilde{x} \quad (x \in X).$$

Denn für $i \in H$ ist

$i \in \beta(\wedge X)$ äquivalent $i \subset \wedge X$
äquivalent $i \subset x$ für alle $x \in X$
äquivalent $i \in \wedge_m \{k;\ k \in H,\ k \subset x\} = \underset{x \in X}{\wedge_m} \tilde{x}$.

$i \in \beta(\vee X)$ äquivalent $i \subset \vee X$
äquivalent Es gibt ein $x_0 \in X$ mit $i \subset x_0$ (da i perfekt)
äquivalent $i \in \underset{x \in X}{\vee_m} \tilde{x}$.

Es folgt, daß β Verbandsisomorphismus ist, wie behauptet wurde.

(β) Ist umgekehrt H beliebig vorgegeben, so ist $\mathfrak{B}(H)$ nach 2.2 m-Verband. Satz 2 folgt nun unmittelbar aus 2.3.

Aus Satz 1 hat man die

3.8. Folgerung. *Für einen glatten Verband* A *sind äquivalent*

(1) A *ist* m-*Verband.*
(2) A *genügt* (D^* 1).

(3) *A ist voll distributiv.*
(4) *Jedes v. i. Element in A ist perfekt.*

Dies gilt also etwa in jedem Verbande mit Minimalbedingung.

3.9. Es ist klar, daß sich die behandelten Begriffsbildungen und Ergebnisse dualisieren lassen. In einem Verbande A, der die zur Glätte duale Eigenschaft (d.h. also Darstellbarkeit jedes Elements als Schnitt voll $\cap$-irreduzibler) besitzt — z.B. in einem Verbande mit Maximalbedingung — sind somit äquivalente Eigenschaften

(1) A ist m-Verband,
(2) A genügt $(D^* 2)$,
(3) A ist voll distributiv

und natürlich ließe sich als (4) noch die zu 3.8, (4), duale Aussage als Eigenschaft der voll $\cap$-irreduziblen Elemente formulieren.

Es läßt sich leicht zeigen, daß eine gegebene „Einbettung" eines m-Verbandes in ein $\mathfrak{P}(m)$ durch Klassenbildung innerhalb der Trägermenge m stets in der Weise „normiert" werden kann, daß sie bis auf Verbandsisomorphie mit der Banddarstellung, der Einbettung $A \to \mathfrak{B}(H) \subset_m \mathfrak{P}(H)$ also, übereinstimmt. Jedoch sei hierauf nicht mehr eingegangen.

§ 4. Der Spezialfall einer vollen Potenzmenge

4.1. Spezialfall eines m-Verbandes A ist der, daß A isomorph dem vollen Verbande $\mathfrak{P}(m)$ wird. Es sei an folgendes Ergebnis aus HERMES [7] erinnert (Satz 24.3): *Die folgenden Eigenschaften eines Verbandes A sind äquivalent:*

(1) *A ist isomorph einer Potenzmenge* $\mathfrak{P}(m)$.
(2) *A ist Boolesch und atomar.*
(3) *A ist Boolesch und genügt dem Gesetze* $\wedge \vee \mathfrak{A} = \vee \wedge \breve{\mathfrak{A}}$ (vgl. 1.1).
(4) *A ist Boolesch und genügt dem Gesetze* $\vee \wedge \mathfrak{A} = \wedge \vee \breve{\mathfrak{A}}$
(wo $\mathfrak{A}$ *eine beliebige Menge von Teilmengen von A ist).*

Als Menge m mit $A \cong \mathfrak{P}(m)$ kann für solch einen Verband A stets die Menge P_A seiner Atome dienen: $A \cong \mathfrak{P}(P_A)$. Die Tatsache, daß A die genannten Eigenschaften hat, wollen wir im folgenden in der Bezeichnungsweise $A \cong \mathfrak{P}(m)$ oder auch $A \cong \mathfrak{P}(P_A)$ zusammenfassen.

Der Verbandsisomorphismus zwischen A und $\mathfrak{P}(P_A)$ wird vermittelt durch die reziproken Abbildungen

$$A \ni a \to \langle a \rangle = \{p;\ p \in P_A,\ p < a\}$$
$$A \ni \vee Q \leftarrow Q \in \mathfrak{P}(P_A)$$

$(\vee\langle a\rangle = a,\ \langle \vee Q\rangle = Q)$. Man sieht leicht, daß $A \cong \mathfrak{P}(m)$ äquivalent ist zu
(5) *A ist* m*-Verband und jedes* $i \in H$ *Atom.*

Wir sagen ferner

4.2. DEFINITION. Sei A ein vollständiger Verband, a beliebig in A und X eine Teilmenge von A. a heißt *direkte Verbindung* der Menge $X \subset_m A$, $a = \vee' X$, wenn

(1) $a = \vee X$,
(2) $\vee Y \cap \vee (X \dot{-} Y) = 0$ für alle $Y \subset_m X$
erfüllt ist.

4.3. *Sei* $A = \mathfrak{P}(P_A)$, *es bestehe also der Verbandsisomorphismus*

$$a \rightleftarrows \langle a \rangle = \{p;\ p \in P_A,\ p < a\} \subset_m P_A$$

($a \in A$, $\langle a \rangle \in \mathfrak{P}(P_A)$). *Dann ist jedes* $a \in A$ *die direkte Verbindung* $a = \vee' \langle a \rangle$; *wegen der Eindeutigkeit der Beziehung zwischen* A *und* $\mathfrak{P}(P_A)$ *besteht* A *also aus den sämtlichen direkten Verbindungen* $\vee' Q$, $Q \subset_m P_A$. *Insbesondere gilt* $1 = \vee' P_A$.

Beweis. Sei $a \in A$. Wir haben $a = \vee \langle a \rangle$. Ist ferner $Y \subset_m \langle a \rangle$, so gilt wegen der vollen Distributivität $\vee Y \cap \vee (\langle a \rangle \dot{-} Y) = \vee (p \cap q)$ (wo $p \in Y$, $q \in \langle a \rangle \dot{-} Y$ ist). Da Y und $\langle a \rangle \dot{-} Y$ leeren Durschschnitt haben, ist stets $p \neq q$, also $p \cap q = 0$. Es folgt $\vee Y \cap \vee (\langle a \rangle \dot{-} Y) = 0$.

4.4. Aus (5) in 4.1 ergibt sich mühelos das Theorem B aus Balachandran [2], welches die Äquivalenz von $A \cong \mathfrak{P}(m)$ zu
(6) *A ist* m*-Verband, und zu jedem* $a \in A$, $a \neq 1$, *gibt es in A ein Element* $b \neq 0$ *mit* $a \cap b = 0$
besagt.

Beweis. Ist (5) erfüllt und $a \neq 1$, so gibt es ein Atom i mit $i \not\leqq a$. Es ist $i \cap a = 0$.

Angenommen, (6) gälte, (5) jedoch nicht. Sei i v. i., aber kein Atom. Sei i^* die Verbindung aller $k \in H$ mit $k \not\geqq i$. Es genügt zu zeigen, daß für jedes $j \in H$ gilt $j \cap i^* \neq 0$. Ist $j \not\geqq i$, so folgt $j < i^*$, $j \cap i^* = j \neq 0$. Sei $j > i$. Da i nicht Atom ist, gibt es ein $k \in H$ mit $k <' i$. Wir haben $j \cap i^* > i \cap k = k \neq 0$.

§ 5. Kettenbedingungen

Der Zusammenhang zwischen einem m-Verbande A und der Halbordnung H seiner v. i. Elemente bewirkt eine Spiegelung zwischen Kettenbedingungen in A und H.

5.1. Sei A ein vollständiger Verband. Für jedes $a \in A$ setzen wir

$n(a) = \vee \{x;\ x \in A,\ x > a\}$, wenn a obere Nachbarn hat,

$n(a) = a$ andernfalls.

Man[2]) definiert dann die *untere Loewy-Reihe* $u_0 \subset u_1 \subset \cdots$ in A:

Definition.

$$u_0 = 0$$

$$u_{\nu+1} = n(u_\nu)$$

$$u_\lambda = \bigvee_{\nu < \lambda} u_\nu \quad \text{für Limesindizes } \lambda$$

wo die Indizes einer wohlgeordneten Indexmenge I entnommen sind).

[2]) Siehe etwa Zassenhaus [10], S. 215, oder auch Baer [1], S. 38.

Es gibt einen ersten Index σ mit $u_{\sigma+1}=u_\sigma$.
Das Ziel dieses Paragraphen ist nun der folgende

5.2. SATZ 3. *Die folgenden Eigenschaften eines* m*-Verbandes A sind äquivalent:*

(1) *Die Halbordnung H der v. i. Elemente von A erfüllt die Minimalbedingung.*
(2) *A ist $\uparrow$-atomar.*
(3) *Jedes $a\in A$, $a\neq 1$ hat obere Nachbarn in A.*
(4) *A besitzt eine bis zum Allelement aufsteigende untere Loewy-Reihe.*
(5) *In A gibt es eine maximale wohlgeordnete Kette von 0 nach 1.*

Der Beweis dieses Satzes ergibt sich aus einer Reihe von Hilfssätzen, die auch für sich von Interesse sein dürften.

5.3. Lemma 1. *Der Verband A sei glatt und modular. Dann gilt für Elemente $a, b\in A$:*

Aus $b<a$ folgt, daß die (nicht leere) Menge $\tilde{a}\div\tilde{b}$ aus lauter unvergleichbaren Elementen besteht. Für jedes $i\in a\div b$ ist $b\cup i=a$. Ist umgekehrt $a=b\cup i$ für ein $i\in\tilde{a}\div\tilde{b}$, das in $\tilde{a}\div\tilde{b}$ minimal ist, so gilt $b<a$.

BEWEIS. In einem glatten Verbande ist die Zuordnung $a\to\tilde{a}$ $(\vee\tilde{a}=a)$ eineindeutig.

(α) Sei $b<a$.

Aus $b<'a$ folgt $\tilde{b}<'_m\tilde{a}$, also die Existenz eines $i\in\tilde{a}\div\tilde{b}$. Man hat $\tilde{b}<_m\widetilde{b\cup i}$, $b<'b\cup i<a$, also $a=b\cup i$.

Für jedes $k\in\tilde{a}\div\tilde{b}$ ist in dieser Weise $a=b\cup k$. Gäbe es ein $k\in\tilde{a}\div\tilde{b}$ mit $k<'i$, also $k<i'$ (s. 1.6), so hätte man $a=b\cup k<b\cup i'<b\cup i=a$ also $b\cup i'=a$. Wegen $i\not\subset b$ gilt $b\cap i<'i$, also $b\cap i<i'$. Hiermit folgt $i=i\cap a=i\cap(b\cup i')=(i\cap b)\cup i'$ (nach dem modularen Gesetz) $=i'$, q.e.a.

Es folgt, daß die $i\in\tilde{a}\div\tilde{b}$ sämtlich maximal in $\tilde{a}$ und minimal in $H\div\tilde{b}$ sind.

(β) Sei $a=b\cup i$ für ein $i\in\tilde{a}\div\tilde{b}$, das in dieser Menge minimal ist.

Es folgt $b<'a$ und $i'<b$, also (wegen $b\cap i<'i$) $i'=b\cap i$. Für ein c mit $b<'c<a$ sei $c\cup i=a$. Wäre $i\not\subset c$, so $i\cap c<'i$, also (da $i'=i\cap b<i\cap c$ gilt) $i\cap c=i'$. Hiermit hätte man $b=b\cup(i\cap b)=b\cup i'=b\cup(i\cap c)=(b\cup i)\cap c$ nach dem modularen Gesetz; also $b=a\cap c=c$ entgegen der Annahme. Also ist $i<c$, $c=a$, und man hat $b<a$.

5.4. Folgerung 1. *In einem glatten modularen Verband ist für Elemente a, b dann und nur dann $b<a$, wenn $a=b\cup i$ gilt für ein $i\in H$, das minimal in der Menge $H\div\tilde{b}$ ist.*

5.5. Folgerung 2. *Für Elemente a, b eines* m*-Verbandes A ist $b<a$ äquivalent mit $a=b\cup i$ für genau ein $i\in H$.*

BEWEIS. Daß die Bedingung hinreicht, ist nach 5.3. klar. Ist umgekehrt $b<a$ und $a=b\cup i=b\cup k$ für Elemente $i, k\in H\div\tilde{b}$ so ergibt sich aus der Perfektheit von i, k, daß aus $i\not\subset b$ folgt $k<i$ und aus $k\not\subset b$ folgt $i<k$, also $i=k$ gilt.

Es ist klar, daß in einem ↑-atomaren[3]) Verbande jedes vom Allelement verschiedene Element obere Nachbarn besitzt. Für bestimmte Verbände läßt sich nun leicht die Umkehrung beweisen:

5.6. Lemma 2. *Der Verband A sei modular und habe zudem die Eigenschaft, daß für jede Kette $K \subset_m A$ und jedes Element $a \in A$ gilt $a \cap \vee K = \vee (a \cap K)$. Dann sind die Aussagen „A ist ↑-atomar" und „jedes $a \in A$, $a \neq 1$, hat obere Nachbarn" gleichwertig.*

(Zum Beispiel erfüllt der Verband aller Normalteiler einer Gruppe die Voraussetzungen dieses Lemmas.)

Beweis. Seien $a, b \in A$ mit $b <' a$. b hat einen oberen Nachbarn n_1, n_1 einen oberen Nachbarn n_2 und so fort; es läßt sich eine maximale wohlgeordnete Kette von b nach 1 bilden:

$$n_\nu < n_{\nu+1}$$

$$n_\lambda = \bigvee_{\nu<\lambda} n_\nu \quad \text{für Limesindizes } \lambda.$$

Aus $b < n_1$ folgt (wegen $b \leq a$, $b \leq n_1$, also $b \leq a \cap n_1$), daß $a \cap n_1 = n_1$ oder $a \cap n_1 = b$ gilt. Im ersten Falle ist $n_1 \subset a$ und nichts mehr zu beweisen.

Sei also $a \cap n_1 = b$. Da es einen Index σ mit $n_\sigma = 1$, $a \cap n_\sigma = a \neq b$ gibt, kann nicht $a \cap n_\nu = b$ für alle Indizes ν sein. Es gibt einen ersten Index μ mit $a \cap n_\mu > b$. μ kann nicht Limesindex sein, denn für Limesindizes λ mit der Eigenschaft „aus $\nu < \lambda$ folgt $n_\nu \cap a = b$" folgt

$$a \cap n_\lambda = a \cap \bigvee_{\nu<\lambda} n_\nu = \bigvee_{\nu<\lambda} (a \cap n_\nu) = \vee b = b.$$

Sei $c = a \cap n_\mu$. Es ist $b \subset c \cap n_{\mu-1} \subset a \cap n_{\mu-1} = b$, also $c \cap n_{\mu-1} = b$. Hieraus folgt weiter $c \not\subseteq n_{\mu-1}$ (da sonst $c \cap n_{\mu-1} = c \neq b$ wäre), also (wegen $c \cup n_{\mu-1} \subset n_\mu$ und $n_{\mu-1} < n_\mu$) die Beziehung $c \cup n_{\mu-1} = n_\mu$. Da für beliebige Elemente x, y eines modularen Verbandes $x \cap y < x$ gleichwertig ist mit $y < x \cup y$ (Hermes [7], § 13, S. 70), folgt aus $n_\mu = n_{\mu-1} \cup c > n_{\mu-1}$, daß $b = n_{\mu-1} \cap c < c$ gilt.

Also ist $c = a \cap n_\mu \subset a$ oberer Nachbar von b unter a.

Zusammen mit 5.4 hat man sofort

5.7. *In einem glatten modularen Verband hat genau dann jedes Element $a \neq 1$ obere Nachbarn, wenn jede der Teilmengen $H \doteq \tilde{a}$, $1 \neq a \in A$, minimale Elemente enthält.*

Genau dann ist A ↑-atomar, wenn jede der Teilmengen $\tilde{a} \doteq \tilde{b}$, $a, b \in A$ mit $b <' a \neq 1$, minimale Elemente enthält.

Gilt zudem in A für beliebige Ketten K und Elemente a die Gleichung $a \cap \vee K = \vee (a \cap K)$, so sind die genannten vier Eigenschaften gleichwertig.

Aus 5.7 ergibt sich insbesondere die Äquivalenz der Eigenschaften (2) und (3) sowie die Implikation „aus (1) folgt (2)" in Satz 3.

5.8. *Ein vollständiger modularer Verband A besitzt genau dann eine untere Loewy-Reihe vom Null- zum Allelement, wenn jedes von 1 verschiedene $a \in A$ obere Nachbarn hat.*

[3]) Siehe 1.7.

BEWEIS. Daß die Bedingung hinreicht, ist klar. Sei umgekehrt die Existenz einer bis zum Allelement aufsteigenden Loewy-Reihe $0=u_0<u_1<\cdots$ $u_\sigma=1$ vorausgesetzt und a ein beliebiges von 1 verschiedenes Element von A.

Aus $a>u_0=0$, $a\not\geqslant u_\sigma=1$ folgt: Es gibt einen ersten Index μ mit $a\not\geqslant u_\mu$. Für Limesindizes folgt aus $u_\nu<a$ für alle $\nu<\lambda$, auch noch $u_\lambda<a$. Also kann μ nicht Limesindex sein.

u_μ ist die Verbindung der oberen Nachbarn von $u_{\mu-1}$ und es ist $u_{\mu-1}<a$. Aus $u_\mu\not<a$ folgt die Existenz eines oberen Nachbarn y von $u_{\mu-1}$ mit $y\not<a$, also $y\cap a<' y$. Man hat dann $u_{\mu-1}<y\cap a<' y$, also $y\cap a=u_{\mu-1}$. Da A modular ist, folgt aus $y\cap a=u_{\mu-1}<y$, daß $y\cup a$ oberer Nachbar von a ist.

5.9. *Ein modularer Verband ist genau dann $\uparrow$-atomar, wenn er eine maximale wohlgeordnete Kette vom Null- zum Allelement besitzt.*

BEWEIS. Die $\uparrow$-Atomarität eines Verbandes bedeutet, daß zwischen je zwei Elementen a, b mit $a>b$ eine maximale wohlgeordnete Kette existiert. In modularen Verbänden aber ist letzteres mit der Existenz einer maximalen wohlgeordneten Kette von 0 nach 1 äquivalent; denn bei Existenz einer solchen Kette läßt sich bekanntlich für jedes Element a die Kette $0<a<1$ zu einer der ersten Ketten isomorphen verfeinern. (s. etwa A. KUROSCH [6]; G. BIRKHOFF [3]).

BEWEIS von Satz 3. Aus 5.7, 5.8, 5.9 ergibt sich für m-Verbände die Gleichwertigkeit der Eigenschaften (2), (3), (4), (5) in Satz 3 und die Tatsache, daß jede von ihnen aus (1) folgt. Zu zeigen bleibt etwa die Implikation „aus (5) folgt (1)".

Sei hierzu $0=a_0<a_1<a_2\ldots a_\nu<a_{\nu+1}\ldots a_\sigma=1$ eine maximale wohlgeordnete Kette vom Null- zum Allelement in A.

Für alle $\nu\leqq\sigma$ gilt nach 5.5. $a_{\nu+1}=a_\nu\cup i$ für genau ein $i\in H$, das mit $i_{\nu+1}$ indiziert werden möge. Jedes $i\in H$ tritt genau einmal als ein solches Ergänzungsglied auf:

Aus $a_\sigma=1=\bigvee H$ nämlich folgt, daß für ein $i\in H$ gilt $i<a_\sigma$. Es gibt einen ersten Index μ mit $i<a_\mu$. μ kann nicht Limesindex sein, denn aus $i<\bigvee_{\nu<\lambda} a_\nu=a_\lambda$ folgt (da i perfekt ist) $i<a_\nu$ für ein $\nu<\lambda$.

Aus $i\not<a_{\mu-1}$, $i<a_\mu$, $a_{\mu-1}<a_\mu$ hat man wegen 5.5 $i=i_\mu$. Der Index μ ist zu i eindeutig bestimmt.

Ist X eine beliebige nicht leere Teilmenge von H, so gibt es einen ersten Index ξ mit $x<a_\xi$ für ein $x\in X$.

Nach demselben Schluß wie oben folgt, daß ξ nicht Limesindex sein kann; es ist $x=i_\xi$. Für ein $y\in H$ mit $y<' x$ folgt $y<a_{\xi-1}$ (da sich aus $y\not<a_{\xi-1}$ ergeben würde $a_{\xi-1}<' a_{\xi-1}\cup y<a_{\xi-1}\cup x=a_\xi$, also $a_{\xi-1}\cup y=a_{\xi-1}\cup x$ entgegen der Eindeutigkeit von $x=i_\xi$). y kann also nach der Auswahl des Index ξ nicht in X liegen; x ist minimal in X.

Hiermit ist Satz 3 bewiesen.

Wir zeigen noch:

5.10. *Die Eigenschaft eines Verbandes A, $\uparrow$-atomarer m-Verband zu sein, vererbt sich auf alle vollständigen Teilverbände von A.*

Beweis. Sei B vollständiger Teilverband von A, b ein beliebiges Element aus B und u das Allelement in B. B ist m-Verband (3.5). Nach Voraussetzung gibt es maximale wohlgeordnete Ketten in A zwischen b und u; durch jedes x mit $b \subset' x \subset u$ läßt sich so eine Kette legen. Sei $\mathfrak{K}$ die Gesamtheit dieser Ketten. Wegen $u \in B$ gibt es in jeder Kette $K \in \mathfrak{K}$ ein Element $b_{\mu(K)}$, welches das erste (in der zu K gehörigen Wohlordnung) von b verschiedene Element aus K ist, das gleichzeitig in B liegt. Sei μ minimal unter den Indizes $\mu(K)$, $K \in \mathfrak{K}$. b_μ liegt in B, und nach Konstruktion kann es kein $x \in B$ mit $b \subset' x \subset' b_\mu$ geben. b_μ also ist in B oberer Nachbar von b.

Insbesondere folgt aus 5.10, daß mit A jedes Intervall $[b, a]$ $(a, b \in A$ beliebig mit $b \subset' a)$ $\uparrow$-atomarer m-Verband ist.

5.11. Auf Grund der engen Verbindung, die zwischen A und H bei einem m-Verbande besteht, könnte man auf den Gedanken kommen, die Minimalbedingung in H impliziere vielleicht sogar die Minimalbedingung in A. (Bekanntlich folgt aus der Endlichkeit der Halbordnung der irreduziblen Elemente eines distributiven Verbandes die Endlichkeit des Verbandes selbst.) Daß dies nicht der Fall ist, zeigt folgendes sehr einfache Beispiel, in dem A sogar voller Potenzmengenverband — Boolesch und atomar — ist: H bestehe aus (etwa abzählbar) unendlich vielen unvergleichbaren Elementen $p_1, p_2, p_3, \ldots, p_i, p_{i+1}, \ldots$, die also alle Atome in A werden. Sicher erfüllt H die Minimalbedingung. Die Bänder $(H \div p_1)$, $(H \div (p_1 \cup_m p_2))$, $(H \div (p_1 \cup_m p_2 \cup_m p_3)), \ldots$ bilden eine unendliche absteigende Kette im Bänderverbande von A.

Es ist klar, daß sich die Begriffsbildungen und Ergebnisse des letzten Paragraphen dualisieren lassen; doch sei hierauf nicht mehr eingegangen.

Literatur

[1] Baer, R.: The double Chain Condition in Cyclic Operator Groups. Amer. J. Math. **69**, 1, 37—45 (1947). — [2] Balachandran, V. K.: A Characterization of $\Sigma\Delta$-Rings of Subsets. Fundamenta Math. **41**, 38—41 (1954). — [3] Birkhoff, G.: Lattice Theory. A.M.S., Coll. Publ. **25**, 2nd ed. (1948). — [4] Birkhoff, G.: Transfinite Subgroup Series. Bull. A.M.S. **40**, 847—850 (1934). — [5] Bruns, G.: Verbandstheoretische Kennzeichnung vollständiger Mengenringe. Archiv d. Math. **10**, 109—112 (1959). — [6] Kurosch, A.: Eine Verallgemeinerung des Jordan-Hölderschen Satzes. Math. Annalen **111**, 13—18 (1935). — [7] Hermes, H.: Einführung in die Verbandstheorie. Berlin, Göttingen, Heidelberg: Springer 1955. — [8] Raney, G. N.: Completely Distributive Complete Lattices. Proc. Amer. Math. Soc. **3**, 677—680 (1952). — [9] Wielandt, H.: Eine Verallgemeinerung der invarianten Untergruppen. Math. Z. **45**, 209—244 (1939). — [10] Zassenhaus, H.: The Theory of Groups. Chelsea, New York 1958.

Frankfurt a. M., Mathematisches Seminar der Universität

(Eingegangen am 23. Juni 1959)

Menzel, W.
Math. Zeitschr. 74, 52–65 (1960)

Über den Untergruppenverband einer Abelschen Operatorgruppe Teil II: Distributive und m-Verbände von Untergruppen einer Abelschen Operatorgruppe

Von
Wolfram Menzel

Einleitung

In Fortsetzung der verbandstheoretischen Untersuchungen in Menzel [12] behandelt diese Arbeit Beziehungen zwischen Eigenschaften einer abelschen Operatorgruppe (g, Ω) und Eigenschaften des Verbandes ihrer zulässigen Untergruppen. Das Thema ist bestimmt durch zwei Eigenschaften dieses Verbandes, nämlich 1. Distributivität, 2. daß der genannte Verband einem vollständigen Teilverbande der Potenzmenge einer Menge verbandsisomorph sei. Operatorgruppen mit endlichem distributiven Ω-Untergruppenverband sind in Behrens [7] näher untersucht worden.

Verbände mit der zweiten Eigenschaft sind näher behandelt in Menzel [12] und werden dort als „m-Verbände" bezeichnet. Nennt man ein Verbandselement „voll $\cup$-irreduzibel", wenn es nicht als Verbindung echt früherer dargestellt werden kann, so ist ein m-Verband A vollständig charakterisiert durch die Halbordnung der in ihm voll $\cup$-irreduziblen Elemente. Ein vollständiger Verband ist genau dann m-Verband, wenn er „glatt" ist (d.h. jedes Verbandselement Verbindung voll irreduzibler ist) und dem einen der beiden unendlich-distributiven Gesetze genügt (s. Menzel [12], Satz 1). Dies bedeutet nunmehr: Ein Verband von Untergruppen einer Gruppe ist genau dann m-Verband, wenn er glatt und distributiv ist (1.7).

In § 1 dieser Arbeit werden die voll-irreduziblen Untergruppen von (g, Ω) charakterisiert als diejenigen, welche zyklisch und „einköpfig" im Sinne von Wielandt [15] sind (d.h. genau eine maximale Ω-Untergruppe besitzen), (Satz 1, 2.3). Weiter ergibt sich (Satz 2, 3.5), daß die Distributivität des Untergruppenverbandes jeder der beiden folgenden Eigenschaften äquivalent ist:

(I) Zu einem beliebigen Paare a, b von Untergruppen gibt es keinen nichttrivialen Homomorphismus zwischen den Faktorgruppen $a-(a\cap b)$ und $b-(a\cap b)$.

(II) Für jedes Untergruppenpaar a, b und jedes Element $\gamma \in a \cup b$ gilt $(a:\gamma)\cup(b:\gamma)=\Omega$ im Verband der Rechtsideale von Ω.

[Hierbei ist $(a:\gamma)$ der „Quotient" $\{\omega;\, \omega\in\Omega,\ \gamma\omega\in a\}$.] Ist der Untergruppenverband sogar glatt und $\uparrow$-atomar im Sinne von Birkhoff [8] (letzteres bedeutet: Zu je zwei Verbandselementen x, y mit $y<' x$ gibt es obere

Nachbarn von y unter x), so läßt sich (I) durch eine schärfere Aussage ersetzen (Satz 4, 4.5). Distributivität impliziert nunmehr, daß für jede Untergruppe a der Gruppe g und jeden Homomorphismus η von a in g gilt $a^{\eta} \subset a$. Für einen glatten, $\uparrow$-atomaren Untergruppenverband von (g, Ω) gilt ferner: Bezeichnet man zu einer voll $\cup$-irreduziblen Untergruppe i von (g, Ω) mit i' die (einzige) maximale Untergruppe von i, so wird der Verband genau dann ein m-Verband, wenn für beliebige voll $\cup$-irreduzible Untergruppen i, k aus der Isomorphie der Faktorgruppen $i - i'$ und $k - k'$ folgt, daß $i \subset k$ oder $k \subset i$ gilt, (Satz 3, 4.4). Als Spezialisierung wird in § 4 eine Verallgemeinerung des Satzes (s. etwa Zassenhaus [*16*], S. 214) bewiesen, nach welchem im Untergruppenverbande einer von ihren minimalen Untergruppen erzeugten Gruppe aus der Distributivität des Verbandes folgt, daß keine verschiedenen Untergruppen einander isomorph sind (Satz 5, 5.2).

Die Betrachtung der Beziehungen zwischen Distributivität des Untergruppenverbandes und Invarianzeigenschaften der Untergruppen bei Homomorphismen geht zum größten Teil auf Anregung von R. Baer zurück. Ferner gehört der folgende von E.-A. Behrens in einer Vorlesung über Ringtheorie gezeigte Satz in diesen Problemkreis: Sei T ein halb-primärer Ring mit Einselement, m ein T-Modul; für je vier T-Untermoduln a, b, c, d, von m mit $a \prec b \subset c \prec d$ gelte $b - a \cong d - c$. Dann ist der Verband der T-Untermoduln von m distributiv. Daß die Distributivität des Untergruppenverbandes mit der oben genannten Eigenschaft (II) gleichbedeutend ist, beruht auf einer Verallgemeinerung (Lemma 3.2) des „Theorem 1" in Suzuki [*14*], welches ein Kriterium dafür darstellt, daß ein Untergruppenpaar „distributives Paar" (vgl. Def. 3.1) ist: "A pair of subgroups A and B forms a distributive pair if and only if for every element $c \in A \cup B$, not in A nor in B, its relative orders with respect to A and B are finite and relatively prime to each other". Der Spezialfall schließlich, daß die Gruppe von ihren minimalen Untergruppen erzeugt wird, ist teilweise bereits in Zassenhaus [*16*] (Appendix B, 3., 4) behandelt — dort allerdings für beliebige (nicht notwendig abelsche) Gruppen, jedoch ohne genaueres Eingehen auf einen Operatorenbereich.

§ 1. Bezeichnungen und Vorbemerkungen

1.1. Gegeben sei eine abelsche Gruppe g mit einem Ring Ω von Rechtsoperatoren. Da keine nicht abelsche Gruppen betrachtet werden, wollen wir nur noch von der „Gruppe g" sprechen. Die Elemente von g werden mit kleinen griechischen, die Untergruppen dieser Gruppe mit kleinen lateinischen Buchstaben bezeichnet. Große lateinische Buchstaben sollen in der Regel für Mengen von Untergruppen verwendet werden.

Der Ring Ω besitze ein Einselement und dieses operiere identisch in g. Ω braucht nicht treu zu sein.

Zu g darf ein (Links-)Operatorenbereich Λ hinzugegeben sein; ist dies der Fall, so sei stets die Λ-Zulässigkeit der Operatoren aus Ω vorausgesetzt.

Zu Untergruppen a, b von g mit $b \subset a$ bezeichne $a - b$ die Faktorgruppe von a nach b.

Wie in MENZEL [12] wird zwischen den verbandstheoretischen Zeichen $\subset, \cap, \cup$ und den Symbolen $\subset_m, \cap_m, \cup_m$ unterschieden, welche mengentheoretisches Enthaltensein, mengentheoretischen Durchschnitt und mengentheoretische Vereinigung bezeichnen.

Für Elemente a, b eines Verbandes bedeute ferner $b \subset' a$, daß $b \subset a$ und $b \neq a$ gilt; ist b „unterer Nachbar" von a, so schreiben wir $b \prec a$. Wir bedienen uns für Schnitte und Verbindungen in einem vollständigen Verbande der abkürzenden Komplexschreibweise $\wedge X$ statt $\bigwedge_{x \in X} x$, usw.

1.2. Es sei Γ der Ring aller Endomorphismen der Gruppe g (ohne Operatoren), G der Verband aller Untergruppen dieser Gruppe. Ist Ξ eine beliebige Teilmenge von Γ, X eine beliebige Teilmenge von G, so sei ferner

$$V\Xi = \{u; u \in G,\ u\xi \subset u \quad \text{für alle} \quad \xi \in \Xi\}$$

und

$$\Phi X = \{\eta; \eta \in \Gamma,\ x\eta \subset x \quad \text{für alle} \quad x \in X\}$$

gesetzt.

Man verifiziert leicht, daß für die Operatoren V und Φ die Operatorgleichungen

$$\Phi V \Phi = \Phi$$

und

$$V \Phi V = V$$

erfüllt sind.

Ist der Operatorenring Ω treu, so kann er stets mit einem Unterring von Γ identifiziert werden. Auch, wenn dies nicht der Fall ist, wollen wir den Verband der Ω-Untergruppen von g mit $V\Omega$ bezeichnen.

1.3. Wie bei MENZEL [12] heiße eine Teilmenge B eines Verbandes A ein *Unterverband* von A, wenn sie bezüglich der durch die Halbordnungsrelation von A in B induzierten Halbordnungsrelation einen Verband bildet; ist der Verband B zudem vollständig, und gilt, daß beliebige Schnitte und Verbindungen in B mit den in A gebildeten Schnitten und Verbindungen übereinstimmen, so nennen wir B einen *vollständigen Teilverband von* A (vgl. HERMES [9], S. 21). Man sieht sofort:

Der Unterverband $V\Omega$ des Verbandes G aller Untergruppen von g ist vollständiger Teilverband von G.

1.4. Zu einer beliebigen Menge Ξ von Rechtsoperatoren der Gruppe g sei $Z\Xi$ der Zentralisator dieser Menge in Γ:

$$Z\Xi = \{\zeta; \zeta \in \Gamma,\ \zeta\xi = \xi\zeta \quad \text{für alle } \xi \in \Xi\}.$$

(Für die leere Menge sei $Z\Xi = \Gamma$ gesetzt.) $Z\Xi$ ist ein Ring, der den identischen Endomorphismus 1 enthält.

Ferner beweist man leicht

1.5. *Ist G der Verband aller Untergruppen der Gruppe g, A vollständiger Teilverband von G und A distributiv, so gilt in A das unendlich-distributive*

Gesetz

$$(D^*1) \qquad a \cap \bigvee_{b \in B} b = \bigvee_{b \in B} (a \cap b),$$

(wo a eine beliebige in A gelegene Untergruppe von g, B eine beliebige Menge in A gelegener Untergruppen von g ist.)

1.6. Wie bei MENZEL [12] heiße ein Element i eines Verbandes A *voll $\cup$-irreduzibel* (v. i.), wenn es nicht als Verbindung echt früherer Elemente dargestellt werden kann; der Verband A heiße *glatt*, wenn jedes seiner Elemente Verbindung von v. i. Verbandselementen ist. Der Verband A werde ein m-*Verband* genannt, wenn er verbandsisomorph einem vollständigen Teilverbande des Potenzmengenverbandes $\mathfrak{P}(m)$ einer Menge m ist. Aus MENZEL [12], Satz 1, zusammen mit 1.3 und 1.5 folgt sofort

1.7. *Der Verband $A = V\Omega$ aller Ω-Untergruppen der Gruppe g ist genau dann* m-*Verband, wenn er glatt und distributiv ist.*

§ 2. Voll irreduzible Untergruppen in $V\Omega$

Gegeben seien g und Ω im Sinne von § 1.

Wir bezeichnen zum Verband $A = V\Omega$ mit H die Halbordnung der voll irreduziblen Untergruppen in A.

2.1. (a) Nach MENZEL [12], 1.6 ist jedes $i \in H$ einköpfig: i enthält genau eine maximale Ω-Untergruppe von g, den „Rumpf" $i' = \bigvee_{k \subset' i} k$. Demgemäß ist $i - i'$ einfache Ω-Gruppe.

(b) Jedes $i \in H$ ist *Ω-zyklisch*: Es gibt ein Element $\iota \in i$ mit $\iota\Omega = i$. Denn wäre $\iota\Omega \subset' i$ für alle $\iota \in i$, so hätte man mit $i = \bigvee_{\iota \in i} \iota\Omega$ eine Darstellung von i als Verbindung echter Ω-Untergruppen.

Wir zeigen, daß die Eigenschaften (a) und (b) auch hinreichen, um die $i \in H$ zu charakterisieren; es gilt sogar die schärfere Aussage:

2.2. *$i \in A$ sei endlich erzeugt und einköpfig. Dann ist i voll irreduzibel in A.*

BEWEIS. Das einköpfige i habe den „Rumpf" i'. Wir zeigen, daß für alle $u \subset a$ gilt $u \subset' i$ *impliziert* $u \subset i'$; hieraus folgt die volle Irreduzibilität von i.

Sei also $i = (\iota_1, \ldots, \iota_n)\Omega$. Aus $u \subset' i$ folgt: Es gibt eine natürliche Zahl k, $1 \leqq k \leqq n$, mit $\iota_k \notin u$. Die Halbordnung X all derjenigen $x \in A$ mit $u \subset x \subset i$, welche mindestens eines der ι_l, $1 \leqq l \leqq n$, nicht enthalten, ist also nicht leer. Für eine Kette $Y \subset_m X$ gilt $w = \vee Y \in X$. (Denn jedes $\xi \in w$ liegt in einem $y \in Y$; lägen also alle ι_l, $l = 1, \ldots, n$, in w, so läge jedes ι_l in einem $y_l \in Y$, mithin — da Y Kette ist — alle ι_l, $l = 1, \ldots, n$, in einem $y \in Y$ entgegen $y \in X$).

Nach dem Zornschen Lemma gibt es in X eine dort maximale Ω-Untergruppe m von g. m ist unterer Nachbar von i, denn aus der Maximalität von m in X folgt, daß für m^* mit $m \subset' m^* \subset i$ gilt $\iota_l \in m^*$ für $l = 1, \ldots, n$ also $m^* = i$.

Wegen der Einköpfigkeit von i ist somit $m = i$, und man hat $u \subset i'$.

Wir haben die Folgerung

2.3. SATZ 1. *Eine Untergruppe $i \subset V\Omega$ ist genau dann voll irreduzibel, wenn sie zyklisch und einköpfig ist.*

§ 3. Distributivität in $V\Omega$

3.1. DEFINITION. Das Paar a, b von Elementen eines Verbandes A heiße ein *distributives Paar in* A, wenn für alle $c \in A$ gilt

$$c \cap (a \cup b) = (c \cap a) \cup (c \cap b).$$

3.2. LEMMA. *Die Untergruppen* $a, b \in A = V\Omega$ *bilden genau dann ein distributives Paar in* A *wenn es zu jedem Element* $\gamma \in a \cup b$ *ein Element* $\mu \in \Omega$ *gibt mit*

$$\gamma\mu \in a$$
$$\gamma(1-\mu) \in b.$$

BEWEIS. 1. a, b sei distributives Paar und $\gamma \in a \cup b$. Speziell für $c = \gamma\Omega$ gilt dann $\gamma\Omega = \gamma\Omega \cap (a \cup b) = (\gamma\Omega \cap a) \cup (\gamma\Omega \cap b)$. Also hat γ die Darstellung $\gamma = \gamma\mu + \gamma\mu^*$ mit $\gamma\mu \in \gamma\Omega \cap a, \gamma\mu^* \in \gamma\Omega \cap b$. Es folgt $\gamma\mu \in a, \gamma(1-\mu) = \gamma - \gamma\mu = \gamma\mu^* \in b$.

2. Die angegebene Bedingung sei für a, b aus A erfüllt. Für jedes $x \in A$, $x < a \cup b$, gilt dann $x = (x \cap a) \cup (x \cap b)$. Denn jedes $\xi \in x$ hat die Form $\xi = \xi\mu + \xi(1-\mu)$ mit $\xi\mu \in x \cap a$, $\xi(1-\mu) \in x \cap b$. Ist $c \in A$ beliebig, so hat man also für $x = c \cap (a \cup b)$ die Gleichung

$$\begin{aligned} c \cap (a \cup b) = x &= (x \cap a) \cup (x \cap b) \\ &= [c \cap (a \cup b) \cap a] \cup [c \cap (a \cup b) \cap b] = (c \cap a) \cup (c \cap b). \end{aligned}$$

3.3. Sind s, t Teilmengen der Gruppe g, so bezeichnen wir durch $(t:s)$ den „Quotienten" $(t:s) = \{\omega; \omega \in \Omega, \sigma\omega \in t$ für alle $\sigma \in s\}$. Ist $t \in V\Omega$, so ist $(t:s)$ Rechtsideal in Ω. Die angegebene Bedingung für die Distributivität eines Untergruppenpaares läßt sich dann in der Form ausdrücken:

Zu jedem $\gamma \in a \cup b$ *ist (im Verband der Rechtsideale von* Ω*)* $(a:\gamma) \cup (b:\gamma) = \Omega$.
(Das folgt sofort aus der Tatsache, daß Ω ein Einselement enthält.)

3.4. Ist im folgenden von einem Homomorphismus einer Gruppe $a \in A = V\Omega$ die Rede, so sei hierunter stets ein Ω-Homomorphismus verstanden. Ist x, y ein Paar von Gruppen, so heiße die Abbildung η ein *Homomorphismus zwischen* x *und* y, wenn η ein Homomorphismus von x in y oder von y in x ist.

Ziel dieses Paragraphen ist nun der folgende

3.5. SATZ 2. *Die folgenden Eigenschaften der* Ω*-Gruppe* g *sind äquivalent*

(1) $A = V\Omega$ *ist distributiv.*
(2) *Für beliebige* $a, b \in A$ *und* $\gamma \in a \cup b$ *gilt* $(a:\gamma) \cup (b:\gamma) = \Omega$.
(3) (2) *gilt für jedes Paar zyklischer* Ω*-Untergruppen* a, b *von* g.
(4) *Zu beliebigen Paaren* $a, b \in A$ *existieren keine nicht trivialen Homomorphismen zwischen* $a - (a \cap b)$ *und* $b - (a \cap b)$.
(5) *Für beliebige* $a, b \in A$ *gilt:*
Aus $a - (a \cap b) \cong b - (a \cap b)$ *folgt* $a = b$.

BEWEIS. (α) Distributivität des Verbandes A meint, daß jedes Paar $a, b \in A$ distributives Paar ist. Die Äquivalenz von (1) und (2) ergibt sich somit unmittelbar aus 3.3.

(β) (2) ist äquivalent (3). Denn ist jedes Paar zyklischer Ω-Untergruppen von g distributives Paar in A, so ist dies für ein beliebiges Paar $a, b \in A$ der Fall: Ein $\gamma \in a \cup b$ nämlich hat die Form $\gamma = \alpha + \beta \in \alpha\Omega \cup \beta\Omega$. Es folgt die Existenz eines $\mu \in \Omega$ mit $\gamma\mu \in \alpha\Omega < a$, $\gamma(1-\mu) \in \beta\Omega < b$, und aus 3.2 somit die Behauptung.

(γ) Daß aus der ersten die vierte (erst recht also die fünfte) Eigenschaft folgt, ergibt sich sofort aus folgendem

3.6. Lemma. *a, b sei ein distributives Paar von Untergruppen in $V\Omega$. Dann ist der Nullhomomorphismus der einzige Homomorphismus zwischen $\bar{a} = a - (a \cap b)$ und $\bar{b} = b - (a \cap b)$.*

Beweis. $a, b \in A$ sei distributives Paar.

1. Man sieht leicht, daß das Distributivitätskriterium 3.2 auch in der Form ausgesprochen werden kann.

„Zu jedem Paar von Elementen $\alpha \in a$, $\beta \in b$ gibt es ein $\nu \in \Omega$ mit $\alpha\nu \in a \cap b$, $\beta(1-\nu) \in a \cap b$."

(Denn die Elemente $\gamma \in a \cup b$ sind ja genau die Elemente der Form $\alpha + \beta$, $\alpha \in a$, $\beta \in b$.)

2. Sei $\bar{\alpha} = \alpha + (a \cap b)$ eine Restklasse aus der Faktorgruppe $\bar{a} = a - (a \cap b)$, η ein Homomorphismus von $\bar{a}$ in $\bar{b}$; wir setzen $\bar{\beta} = \bar{\alpha}^\eta = \beta + (a \cap b)$ (wo $\beta \in b$ ein Repräsentant der Restklasse $\bar{\beta}$ ist). Das in der unter 1. abgeleiteten Form des Distributivitätskriteriums genannte Element $\nu \in \Omega$ mit $\alpha\nu \in a \cap b$, $\beta(1-\nu) \in a \cap b$ bildet jedes Element der Restklasse $\bar{\alpha} = \alpha + (a \cap b)$ in $a \cap b$ ab, und dasselbe tut $1-\nu$ mit jedem Element der Restklasse $\bar{\beta}$. Es folgt also

$$\bar{\alpha}\nu = \bar{0},$$

$$\bar{\beta}(1-\nu) = \bar{0}$$

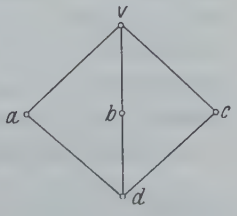
und wir haben

$$\bar{\alpha}^\eta = \bar{\beta} = \bar{\beta}(1-\nu) + \bar{\beta}\nu = \bar{0} + \bar{\alpha}^\eta\nu = \bar{\alpha}^\eta\nu = (\bar{\alpha}\nu)^\eta = \bar{0}^\eta = \bar{0}.$$

(δ) Es bleibt zu zeigen, daß in einem nicht distributiven Verbande $A = V\Omega$ die in 3.5 an letzter Stelle genannte Eigenschaft nicht erfüllt ist. Bekanntlich (Hermes [9], Satz 9.3) enthält ein modularer, nicht distributiver Verband A einen Teilverband der Form

$$a \cup b = b \cup c = c \cup a = v$$

$$a \cap b = b \cap c = c \cap a = d.$$



(Wegen $c \cap (a \cup b) = c \neq d = (c \cap a) \cup (c \cap b)$ ist a, b nicht distributives Paar.) Es ist nach dem zweiten Isomorphiesatz

$$a - (a \cap b) = a - (a \cap c) \cong (a \cup c) - c = (b \cup c) - c \cong b - (b \cap c) = b - (a \cap b).$$

Hiermit ist Satz 2 bewiesen.

Aus Satz 2 folgt insbesondere, daß in distributivem A keine von Null verschiedenen $a, b \in A$ mit $a \cap b = 0$ zueinander isomorph sein können; speziell sind keine verschiedenen Atome $p, q \in A$ isomorph.

Dies Ergebnis steht — formuliert noch unter der Voraussetzung, daß Ω ein „halbprimärer" Ring sei — bereits in BEHRENS [3], § 1, Satz 1.

3.7. Folgerung 1. *Der Verband $A = V\Omega$ sei glatt. A ist genau dann ein* m*-Verband, wenn eine der Eigenschaften* (1) *bis* (5) *aus Satz 2 erfüllt ist* (s. 1.6).

3.8. Folgerung 2. *Jede der Eigenschaften* (1) *bis* (5) *aus Satz 2 ist (notwendig und) hinreichend dafür, daß jedes homomorphe Bild von g distributiven Ω-Untergruppenverband besitzt.*

(Denn der Ω-Untergruppenverband eines homomorphen Bildes von g ist einem vollständigen Teilverband von A verbandsisomorph; auf einen solchen aber vererbt sich die Distributivität von A.)

In einem (abstrakten) Ringe Ω mit Einselement ist die additive Gruppe Ω zyklische Ω-Gruppe mit den Rechtsidealen als zulässigen Untergruppen. Die Gesamtheit der Ω-homomorphen Bilder von Ω^+ ist die Gesamtheit der zyklischen Ω-Gruppen.

Wir haben als

3.9. Folgerung 3. *Für einen Ring Ω mit Einselement sind äquivalente Eigenschaften*

(1) *Jede zyklische Ω-Gruppe hat distributiven Ω-Untergruppenverband.*

(2) *Der Verband der Rechtsideale von Ω ist distributiv.*

(3) *Für jedes Paar von Rechtsidealen [oder jedes Paar von Rechts-Hauptidealen] P, Σ in Ω und jedes $\omega \in \mathsf{P} \cup \Sigma$ gilt*

$$(\mathsf{P} : \omega) \cup (\Sigma : \omega) = \Omega$$

im Verbande der Rechtsideale von Ω.

(4) *Für ein beliebiges Paar P, Σ von Rechtsidealen in Ω gibt es keinen nichttrivialen Ω-Homomorphismus [keinen Ω-Isomorphismus, außer wenn $\mathsf{P} = \Sigma$ ist] zwischen $\mathsf{P} - (\mathsf{P} \cap \Sigma)$ und $\Sigma - (\mathsf{P} \cap \Sigma)$.*

§ 4. m-Verbände $V\Omega$

4.1. Zu den v. i. (einköpfigen) Gruppen $i \in H$ nennen wir die einfache Faktorgruppe $\bar{i} = i - i'$ den *Kopf* von i. Die $i \in H$ lassen sich in Klassen solche mit isomorphen Köpfen einteilen. Wir zeigen

4.2. *In einem distributiven Verbande $A = V\Omega$ gilt für voll irreduzible Untergruppen $i, k \in H$, daß aus $\bar{i} \cong \bar{k}$ folgt $i < k$ oder $k < i$.*

Zum Beweise dient der

4.3. Hilfssatz. *Sei $A = V\Omega$, $b \in A$ und $i \in H$ mit $i \not\subset b$, $i' < b$. Dann besteht mit $a = b \cup i$ die Ω-Isomorphie $a - b \cong \bar{i}$.*

BEWEIS. Aus den Voraussetzungen folgt $i' < i \cap b$; andererseits $i \cap b < i$, also $i \cap b < i'$. Man hat $i \cap b = i'$ und damit $a - b = (b \cup i) - b \cong i - (b \cap i) =$

Beweis von 4.2. Angenommen, es gäbe $i, k \in H$ mit $\bar{i} \cong \bar{k}$, $i \not\subset k$, $k \not\subset i$. Dann folgt

$$i \cap k \subset' i, \qquad i \cap k \subset' k,$$

also

$$i \cap k \prec i', \qquad i \cap k \prec k'.$$

Sei $d = i' \cup k'$, $a = d \cup i$, $b = d \cup k$. Man hat $i \not\subset d$, $k \not\subset d$, und weiter $a \cap b = (d \cup i) \cap (d \cup k) = d \cup (i \cap k) = d$.

Aus 4.3 folgt dann (mit d statt dem dortigen b): $a - (a \cap b) = a - d \cong \bar{i} \cong \bar{k} \cong b - d = b - (a \cap b)$, also nach Satz 2 die Nichtdistributivität von A.

4.2. bedeutet (in unserem Falle abelscher Operatorgruppen) eine Verallgemeinerung des Satzes von Zassenhaus [*16*], S. 214, nach welchem in einer von ihren minimalen Untergruppen erzeugten Gruppe mit distributivem Untergruppenverband keine zwei minimalen Untergruppen isomorph sind.

Unter Zusatzvoraussetzungen läßt sich nun auch die Umkehrung von 4.2 beweisen:

Wie in § 1 bereits erwähnt wurde, nennen wir einen vollständigen Verband *glatt*, wenn jedes seiner Elemente Verbindung voll irreduzibler ist; ein Verband heißt ein m-Verband, wenn er in den Potenzmengenverband $\mathfrak{P}(m)$ einer Menge m vollständig eingebettet werden kann (vgl. 1.6). Weiter nennen wir nach Birkhoff [*8*] einen Verband *↑-atomar*, wenn es zu je zwei Elementen $a, b \in A$ mit $b \subset' a$ obere Nachbarn von b unter a gibt.

Hiermit nun gilt:

A sei glatt und ↑-atomar. Für $i, k \in H$ gelte stets, daß $\bar{i} \cong \bar{k}$ impliziert $i \subset k$ oder $k \subset i$. Dann ist A distributiv.

Beweis. Wir wollen wie in Menzel [*12*] die folgenden verbandstheoretischen Bezeichnungen gebrauchen:

Zu $x \in A$ sei $\tilde{x} = \{i;\ i \in H,\ i \subset x\}$; zu zwei Verbandselementen $x, y \in A$ mit $y \subset x$ sei $[y, x]$ das „Intervall" $\{z;\ z \in A,\ y \subset z \subset x\}$.

Angenommen, A wäre nicht distributiv, enthielte also nach Satz 2 Elemente a, b, $a \neq b$, mit $a - b \cong b - d$ (wo $a \cap b = d$ gesetzt ist). σ sei der verbindende Isomorphismus. σ bewirkt einen Verbandsisomorphismus σ_0 der Intervalle $[d, a]$ und $[d, b]$.

Wegen der ↑-Atomarität von A gibt es obere Nachbarn von d unter a bzw. unter b, und zu jedem m mit $d \prec m \subset a$ gehört eineindeutig ein $n = m^{\sigma_0}$, $d \prec n \subset b$, mit $(m - d)^{\sigma} = n - d$.

Da $d = a \cap b$ maximal ist mit der Eigenschaft $d \subset a$ und $d \subset b$, folgt $m \neq n$. Nach Menzel [*12*], 5.3 gilt dann[1]: Es ist $m = d \cup i$ für ein $i \in H$, das minimal in $H \div \tilde{d}$ ist, und in gleicher Weise $n = d \cup k$ für ein $k \in H$, k minimal in $H - \tilde{d}$,

[1]) Der hier interessierende Teil des dort bewiesenen Lemmas lautet: Der Verband A sei glatt und modular, es seien $a, b \in A$ Elemente aus A mit $b \prec a$. Dann besteht die nicht leere Menge $\tilde{a} \div \tilde{b} = \{i;\ i \in H,\ i \subset a,\ i \not\subset b\}$ aus lauter unvergleichbaren Elementen, und für jedes $i \in \tilde{a} \div \tilde{b}$ ist $a = b \cup i$.

und weiter $i \not\subset k$, $k \not\subset i$. Wegen der Minimalität von i gilt $i' \subset d$, also $i' = i' \cap d \subset i \cap d$ andererseits ist $i \not\subset d$, $i \cap d \subset' i$, also $i \cap d \subset i'$, mithin $i \cap d = i'$. Analog hat man $k \cap d = k'$.

Es folgt:

$$i - i' = i - (i \cap d) \cong (d \cup i) - d = m - d \cong n - d$$
$$= (d \cup k) - d \cong k - (k \cap d) = k - k',$$

womit die Behauptung bewiesen ist.

Aus 4.3 und dem eben Bewiesenen ergibt sich also zusammen mit 1.7

4.4. SATZ 3. *Der Verband $A = V\Omega$ sei glatt und $\uparrow$-atomar. A ist genau dann* m*-Verband, wenn für beliebige in A v. i. Untergruppen $i, k \in A$ aus $\bar{i} \cong \bar{k}$ folgt $i \subset k$ oder $k \subset i$.*

(Man vgl. hierzu MENZEL [*12*], § 5, Satz 3.)

In einem m-Verband A ist nach MENZEL [*12*], § 5, Satz 3 die $\uparrow$-Atomarität von A mit der Minimalbedingung für H gleichwertig. Untergruppen a in einem $\uparrow$-atomaren m-Verband $A = V\Omega$ haben nun noch eine Invarianzeigenschaft bei Homomorphismen, die unter der Voraussetzung der Distributivität allein nicht bewiesen werden konnte:

4.5. SATZ 4. *A sei $\uparrow$-atomarer* m*-Verband. Sei ferner a aus A und η ein Homomorphismus von a in g. Dann ist $a^\eta \subset a$.*

BEWEIS. Man sieht zunächst, daß man sich beim Beweis auf voll irreduzible $a = i \in H$ beschränken kann. Denn ist die Behauptung für solche gezeigt, so folgt für beliebiges $a \in A$

$$a^\eta = \left(\bigvee_{i \in \tilde{a}} i\right)^\eta = \bigvee_{i \in \tilde{a}} i^\eta \subset \bigvee_{i \in \tilde{a}} i = a.$$

Wäre die Menge der $i \in H$, für welche der Satz falsch ist, nicht leer, so gäbe es ein $f \in H$, das minimal ist mit der Eigenschaft: Es gibt einen Homomorphismus η von f in g mit $f^\eta \not\subset f$. Aus der Minimalität von f folgt für alle $k \in H$ mit $k \subset' f$, daß $k^\eta \subset k$ gilt, — somit $f'^\eta \subset f'$.

η induziert einen Homomorphismus η_0 von $f - f'$ auf $f^\eta - f'^\eta$; dieser kann wegen $f^\eta \not\subset f'^\eta$ nicht der Nullhomomorphismus sein — aus der Einfachheit von $f - f'$ folgt also, daß er Isomorphismus ist: $f^\eta - f'^\eta \cong f - f'$.

Im Verbande der Untergruppen von $g - f'^\eta$, welcher gleichzeitig mit A den Voraussetzungen des Satzes genügt, ist (wegen $f \in H$) $f - f'^\eta$ voll irreduzibel und es ist $f^\eta - f'^\eta \not\subset f - f'^\eta$ (da $f'^\eta \not\subset f$); $f^\eta - f'^\eta$ ist wegen der eben abgeleiteten Isomorphie Atom in diesem Verbande: Es folgt $f - f'^\eta \not\subset f^\eta - f'^\eta$ und $f^\eta - f'^\eta \cong f - f' \cong (f - f'^\eta) - (f' - f'^\eta)$ entgegen der Aussage von Satz 3.

Aus Satz 4 hat man sofort als

4.6. Folgerung 1. *In einem $\uparrow$-atomaren* m*-Verbande $A = V\Omega$ sind keine zwei verschiedenen Gruppen Ω-isomorph.*

4.7. Folgerung 2. *$A = V\Omega$ sei $\uparrow$-atomarer* m*-Verband. Dann ist jedes $a \in A$ „Ω-vollinvariant", d.h. $Z\Omega$-Gruppe.*

(Hierbei ist $Z\Omega$, wie in § 1 definiert, der Zentralisator von Ω im Ringe Γ aller Endomorphismen der Gruppe g ohne Operatoren.)

Die Aussage 4.7 läßt sich auch (in der in 1.2 eingeführten Terminologie) in der Form $V\Omega <_m VZ\Omega$ schreiben. Wegen $V\Phi V\Omega = V\Omega$ (1.2) ist nun auch $\Omega^* = \Phi V\Omega = \Phi A$ ein A „definierender" Ring: $V\Omega^* = A$. Nach Definition von ΦA folgt also unter den Voraussetzungen von Satz 4: $Z\Omega^* <_m \Phi A = \Omega^*$; $Z\Omega^*$ liegt also im Zentrum des Ringes Ω^*, und wir haben aus Satz 4 die

4.8. Folgerung 3. *$A = V\Omega$ sei $\uparrow$-atomarer* m-*Verband. Dann ist der Zentralisator des Ringes ΦA ein kommutativer Ring.*

Noch eine letzte Folgerung aus Satz 4 sei genannt:

Sei g die additive Gruppe Ω^+ eines („abstrakten") Ringes Ω, (A also der Verband der Rechtsideale von Ω). Linksmultiplikation der $\omega \in \Omega^+$ mit einem $\lambda \in \Omega$ bedeutet einen Endomorphismus

$$\omega \to \lambda\omega \qquad (\omega \in \Omega^+)$$

von Ω^+, und dieser ist wegen $\lambda(\omega\varrho) = (\lambda\omega)\varrho$ $(\varrho \in \Omega)$ ein Ω-Endomorphismus. Somit ergibt sich

4.9. Folgerung 4. *Ω sei ein Ring mit Einselement. Der Verband der Rechtsideale von Ω sei $\uparrow$-atomarer* m-*Verband. Dann ist jedes Rechtsideal in Ω zweiseitig.*

4.10. Daß es in Satz 4 nicht genügt, die Distributivität von A vorauszusetzen, zeigt das folgende Beispiel:

g sei die additive Gruppe der rationalen Zahlen, A der Verband aller ihrer Untergruppen (also etwa $\Omega =$ Ring der ganzen Zahlen). Man rechnet leicht nach, daß A distributiv ist. Wir zeigen, daß g keine v. i. Untergruppen enthält; also sicher nicht glatt ist.

Nach Satz 1 müßte eine v. i. Untergruppe zyklisch sein, etwa $= \{\varrho\}$. Seien π, π' zwei verschiedene Primzahlen. Die Gruppen $\{\varrho\,\pi\}$, $\{\varrho\,\pi'\}$ sind echt in $\{\varrho\}$ enthalten. Es ist $(\pi, \pi') = 1$, also $1 = \pi\xi + \pi'\xi'$ (ξ, ξ' ganze Zahlen), und

$$\varrho = \varrho \cdot 1 = \varrho\,\pi\,\xi + \varrho\,\pi'\,\xi' \in \{\varrho\,\pi\} \cup \{\varrho\,\pi'\}.$$

Also ist $\{\varrho\}$ Verbindung zweier echter Untergruppen.

Ordnet man jeder rationalen Zahl ϱ die Zahl $\varrho^\eta = \varrho/2$ zu, so ergibt sich ein Endomorphismus η von g. Er bildet die Untergruppe der ganzen Zahlen nicht in sich ab.

Es ist dem Verfasser nicht bekannt, ob man beim Beweise von Satz 4 ohne die $\uparrow$-Atomarität von A auskommen kann.

§ 5. Spezialisierung auf Gruppen, die ihr eigener Sockel sind

Wir spezialisieren auf den Fall, daß die Gruppe g ihr eigener Ω-Sockel ist, d.h. von ihren einfachen Ω-Untergruppen erzeugt wird.

5.1. Sei zunächst daran erinnert, daß in diesem Falle die Distributivität von A jeder der folgenden Eigenschaften äquivalent ist:

(1) A ist Boolesch und atomar[2]).

(2) A ist verbandsisomorph einer vollen Potenzmenge $\mathfrak{P}(m)$. (Wir schreiben $A \cong \mathfrak{P}(m)$. Als m kann stets die Menge P_A der Atome in A genommen werden.) A besteht dann genau aus den sämtlichen „direkten Verbindungen" — nunmehr direkten Summen im gruppentheoretischen Sinne — $\bigvee' Q$, $Q <_m P$.

(3) A ist $\mathfrak{m}$-Verband und jedes $i \in H$ Atom. (Insbesondere erfüllt H die Minimalbedingung, ist A also nach MENZEL [12], Satz 3, $\uparrow$-atomar.)

Wir zeigen

5.2. SATZ 5. *Die Gruppe g sei von ihren minimalen Ω-Untergruppen erzeugt. Dann sind äquivalent*

(1) *A ist distributiv.*

(1') *$A \cong \mathfrak{P}(P_A)$, und A besteht aus den sämtlichen direkten Summen $\sum' Q$ mit $Q <_m P_A$.*

(2) *Keine zwei Atome in A sind als Ω-Gruppen isomorph.*

(2') *Für jedes $a \in A$ und jeden Homomorphismus η von a in g gilt $a^\eta < a$.*

(3) $g = \sum' P_A$ [3]).

(3') *Jedes $a \in A$ ist eindeutig als direkte Summe einer Menge von Atomen in A dargestellt.*

(Die Bezeichnung ist so gewählt, daß die Implikation „aus (n') folgt (n)" trivial ist.)

BEWEIS. (α) Die Äquivalenz von (1), (1'), (2), (2') ist klar nach 5.1 und Satz 4.

(β) Aus (1') folgt (3'). Sei also A Boolesch, $a \in A$, $a = \bigvee X$ mit $X <_m P_A$. Für jedes $x_0 \in X$ gilt dann $x_0 \cap a = x_0 \cap \bigvee X = \bigvee_{x \in X} (x_0 \cap x) = x_0$. Es folgt $x_0 < a$. Für ein $p \in P_A$ mit $p < a = \bigvee X$ gilt andererseits nach MENZEL [12], 1.4, $p \in X$. Also muß X die zu a eindeutig bestimmte Menge $\tilde{a} = \{p;\ p \in P_A,\ p < a\}$ sein.

(γ) (3') impliziert (3) ist trivial.

(δ) Aus (3) folgt (1):

Ist A nicht distributiv, so besitzt es zwei isomorphe Atome p, q; sei $q = p^\sigma$.

Sei $r = \{\alpha + \alpha^\sigma;\ \alpha \in p\}$. Es ist $r \neq 0$ und (wegen der Ω-Zulässigkeit von σ) $r \in A$. Ferner gilt $p \cup r = q \cup r = p \cup q$. Für ein $\delta \in p \cap r$ folgt $\delta = \alpha + \alpha^\sigma \in p$, also $\alpha^\sigma \in p$, $\alpha^\sigma \in p \cap q = 0$, $\alpha = 0$, $\delta = 0$. Wir haben $p \cap r = 0$ und analog $q \cap r = 0$. Mit $v = p \dotplus q$ ergibt sich also, daß v die verschiedenen Darstellungen

$$v = p \dotplus q = p \dotplus r = q \dotplus r$$

als direkte Summe von Atomen hat. Also kann die Verbindung $g = \bigvee P_A$ nicht direkte Summe sein. (Teil (δ) des Beweises ist analog dem von BEHRENS in [7] beim Beweis des dortigen Satzes 1 angewandten Schlußverfahren).

[2]) Ein Verband A heißt „atomar", wenn es zu jedem $a \in A$, $a \neq 0$, ein Atom (d.h. ein minimales Verbandselement) p mit $p < a$ gibt.

[3]) Wir gebrauchen für die direkte Summe die abkürzende Schreibweise $\sum' P_A$ statt $\sum'_{p \in P_A} p$

Die folgenden Aussagen stellen eine Art Umkehrung von Satz 5 dar:

5.3. SATZ 6.

(I) *Sei* $g=\sum' P$ *eine beliebige direkte Zerlegung der Gruppe* g *(ohne Operatoren) in Untergruppen* $p\in P$. *Dann gilt*

(a) *Die sämtlichen direkten Teilsummen* $\sum' Q$, $Q\subset_m P$ *bilden einen Booleschen atomaren Verband* $A\cong\mathfrak{P}(P)$, *und dieser ist vollständiger Teilverband des Verbandes* G *aller Untergruppen von* g.

(b) *Es gibt einen Ring* $\mathsf{T}\subset_m\Gamma$, *so daß* $A=V\mathsf{T}$ *wird.*

(II) *Sei* A *vollständiger Teilverband des Untergruppenverbandes* G *der Gruppe* g *(ohne Operatoren) und* $A\cong\mathfrak{P}(m)$. *Dann ist* $g=\sum' P$, *wo* P *die Menge der Atome von* A *ist.* A *besteht aus den sämtlichen direkten Teilsummen* $\sum' Q$, $Q\subset_m P$, *und es gibt einen Ring* $\mathsf{T}\subset_m\Gamma$ *mit* $A=V\mathsf{T}$.

(III) *Als Ring* T *in* (I) *und* (II) *kann man den Zentralisator der Menge* E, *welche aus den zur genannten direkten Zerlegung von* g *gehörigen Zerlegungsendomorphismen besteht, wählen.*

BEWEIS. *Zu* (I):

(a) Ist ohne weiteres klar: Jedem $a\in A$ ordne man die Menge $\langle a\rangle=\{p;\ p\in P,\ p\subset a\}$ zu.

(b) Zu jedem $p\in P$ gehört der Zerlegungsendomorphismus $\varepsilon_p\in\Gamma$, welcher jedes $\gamma\in g$, $\gamma=\gamma_{p_1}+\cdots+\gamma_{p_n}$ $(\gamma_{p_i}\in p_i\in P)$ auf seine p-Komponente γ_p abbildet. Sei $\mathsf{E}=\{\varepsilon_p;\ p\in P\}$. E ist eine Menge orthogonaler Idempotente in Γ. Wir zeigen $V\mathsf{E}=A$. Die $p\in P$ sind E-zulässig, und damit ist es auch jede Summe $\sum' Q$, $Q\subset_m P$; es folgt $V\mathsf{E}\subset_m A$. Ist andererseits $x\in G$, $x\notin A$, so gibt es ein $\xi\in x$ und ein $p\in P$ mit $\xi_p\notin x$; man hat $x\varepsilon_p\notin x$, $x\notin V\mathsf{E}$, also $V\mathsf{E}\subset_m A$.

Sei $\mathsf{T}=Z\mathsf{E}$ der Zentralisator der Menge E in Γ. Aus der Orthogonalität der $\varepsilon\in\mathsf{E}$ folgt sofort $\mathsf{E}\subset_m\mathsf{T}$, also $V\mathsf{T}\subset_m V\mathsf{E}=A$. Für ein $\alpha\in a$, $\alpha=\alpha\varepsilon_1+\cdots+\alpha\varepsilon_n$, und ein $\tau\in\mathsf{T}$ gilt andererseits $\alpha\tau=\alpha\tau\varepsilon_1+\cdots+\alpha\tau\varepsilon_n$ (wegen $\tau\in Z\mathsf{E}$) mit $\alpha\tau\varepsilon_i\in p_i\subset a$, also $\alpha\tau\in a$. Es folgt $A\subset_m V\mathsf{T}$, und damit $A=V\mathsf{E}=V\mathsf{T}$.

Zu (II) *und* (III). Nach Definition eines vollständigen Teilverbandes von G enthält ein solcher das Allelement g von G (s. HERMES [9], S. 29). Es folgt die direkte Zerlegung $g=\sum' P$, und die übrigen Behauptungen ergeben sich nun aus (I).

Über den Ring T nun läßt sich noch etwas mehr sagen:

5.4. *Sei* $g=\sum' P$ *eine direkte Zerlegung der Gruppe* g, $\mathsf{T}=Z\mathsf{E}$ *der Zentralisator der zu ihr gehörigen Menge von Zerlegungsendomorphismen,* $A=V\mathsf{T}$.

Dann gilt $\mathsf{T}=\Phi A=\Phi P$ (s. 1.2).

BEWEIS. Wegen $P\subset_m A$ ist trivialerweise $\mathsf{T}\subset_m\Phi V\mathsf{T}=\Phi A\subset_m\Phi P$. Sei andererseits $\varphi\in\Phi P$, also $p\varphi\subset p$ für alle $p\in P$. Für beliebiges $\gamma\in g$, $\gamma=\gamma\varepsilon_{p_1}+\cdots+\gamma\varepsilon_{p_n}$, und beliebiges $p\in P$ folgt dann

$$\begin{aligned}\gamma\varphi\varepsilon_p&=\gamma\varepsilon_{p_1}\varphi\varepsilon_p+\cdots+\gamma\varepsilon_{p_n}\varphi\varepsilon_p\\&=\gamma\varepsilon_p\varphi\varepsilon_p\\&=\gamma\varepsilon_p\varphi\quad(\text{da }\gamma\varepsilon_p\varphi\in\varphi\subset p).\end{aligned}$$

φ ist also mit jedem $\varepsilon_p \in \mathsf{E}$ vertauschbar, $\varphi \in \mathsf{ZE} = \mathsf{T}$. Hieraus folgt die Behauptung.

Bei gegebener Zerlegung $g = \sum' P$, gegebener Untergruppenmenge P also, läßt sich A auch noch etwas anders charakterisieren:

Ist allgemein C ein vollständiger Verband, M eine Teilmenge von C, so gibt es stets einen eindeutig bestimmten kleinsten vollständigen Teilverband von C, der M enthält. Wir bezeichnen diesen *„von M in C erzeugten" vollständigen Teilverband* mit $[M]_C$.

Man sieht dann sofort, daß $A = [P]_G$ wird. Denn $[P]_G$ muß einerseits alle Verbindungen $\vee Q$, $Q <_m P$, also A enthalten; andererseits ist A vollständiger Teilverband von G und enthält P.

Insgesamt haben wir das folgende Ergebnis erhalten:

5.5. SATZ 7. *Unter den Voraussetzungen zu Satz* 6, (I) *oder* (II), *gilt für den Verband* A:

$$A = V\,\Phi\,A,$$

für den Ring $\mathsf{T} = \mathsf{ZE}$:

$$\mathsf{T} = \Phi\,V\,\mathsf{T}.$$

Es bestehen nämlich eineindeutige reziproke Beziehungen zwischen

1. *den vollständigen Teilverbänden* A *von* G *mit* $A \cong \mathfrak{P}(m)$;

2. *den direkten Zerlegungen* $g = \sum' P$ *der Gruppe* g, *und*

3. *denjenigen Unterringen* T *von* Γ, *welche Zentralisatoren eines Orthogonalsystems* $\mathsf{E} <_m \Gamma$ *von Idempotenten mit* $g = \bigvee_{\varepsilon \in E} g\,\varepsilon$ *sind.*

Hierbei ist zu gegebenem A

$$P = P_A \quad \textit{(Menge der Atome in } A\textit{)}$$

$$\mathsf{T} = \Phi\,A$$

zu gegebener Zerlegung $g = \Sigma' P$, *also gegebenem* P *bzw. gegebenem Orthogonalsystem* E

$$\mathsf{T} = \mathsf{ZE} = \Phi\,V\,P$$

$$A = V\,\mathsf{E} = [P]_G = \{\textstyle\sum' Q;\ Q <_m P\}$$

zu gegebenem Ringe T

$$A = V\,\mathsf{T}$$

$P =$ *Menge der* T*-einfachen Untergruppen von* g.

Wir haben noch die triviale Folgerung:

5.6. *Hat der Verband* $A = V\Omega$ *die Eigenschaft* $A \cong \mathfrak{P}(m)$, *so ist* Ω *im Zentralisator* $\mathsf{T} = \mathsf{ZE}$ *enthalten.*

BEWEIS. Es ist $\Omega <_m \Phi V \Omega = \Phi A = \mathsf{T}$.

Literatur

[1] Baer, R.: Linear Algebra and Projective Geometry. New York: Ac. Press Inc. 1952. — [2] Baer, R.: Automorphism Rings of Abelian Operator Groups. Annals of Math. **44**, 192—226 (1943). — [3] Baer, R.: Endomorphism Rings of Operator Loops. Trans. A.M.S. **61**, 517—529 (1947.) — [4] Baer, R.: A Unified Theory of Projective Spaces and Finite Abelian Groups. Trans. A.M.S. **52**, 283—345 (1942). — [5] Behrens, E. A.: Zweiseitige Ideale in Algebren endlichen Ranges. Math. Annalen **132**, 95—105 (1956). — [6] Behrens, E. A.: Algebren mit vorgeschriebenem endlichem distributivem Idealverband. Math. Annalen **133**, 79—90 (1957). — [7] Behrens, E. A.: Eine Charakterisierung der T-Moduln mit distributivem Untermodulverband bei halbprimärem T. Archiv d. Math. **8**, 258—273 (1957). — [8] Birkhoff, G.: Lattice Theory. A.M.S. Coll. Publ. **25**, 2nd ed. (1948). — [9] Hermes, H.: Einführung in die Verbandstheorie. Berlin, Göttingen, Heidelberg: Springer 1955. — [10] Jacobson, N.: Structure of Rings. A.M.S. Coll. Publ. **37**, (1956). — [11] Kaplansky, I.: Infinite Abelian Groups. Univ. Mich. Press 1956. — [12] Menzel, W.: Über den Untergruppenverband einer Abelschen Operatorgruppe. Teil I: $\mathfrak{m}$-Verbände. Math. Z. **74**, 39—51 (1960). — [13] Specht, W.: Gruppentheorie. Berlin, Göttingen, Heidelberg: Springer 1957. — [14] Suzuki, M.: Structure of a Group and its Lattice of Subgroups. Berlin, Göttingen, Heidelberg: Springer 1956. — [15] Wielandt, H.: Eine Verallgemeinerung der invarianten Untergruppen. Math. Z. **45**, 209—244 (1939). — [16] Zassenhaus, H.: The Theory of Groups. Chelsea, New York 1958.

Frankfurt a. M., Mathematisches Seminar der Universität

(Eingegangen am 23. Juni 1959)

COHEN, E.
Math. Zeitschr. 74, 66–80 (1960)

Arithmetical functions associated with the unitary divisors of an integer

By
ECKFORD COHEN

1. INTRODUCTION. A divisor $d>0$ of the positive integer n will be called *unitary* if $d\delta=n$, $(d,\delta)=1$, while the divisors d, δ together will be called *complementary* divisors of n. In this paper we consider the *unitary convolution*,

$$f(n)=\sum_{\substack{d\delta=n\\(d,\delta)=1}} g(d)\,h(\delta), \tag{1.1}$$

of arithmetical functions $g(n)$, $h(n)$, it being understood that the summation in (1.1) is extended over the totality of ordered pairs of complementary unitary divisors of n.

The following terminology and notation will be needed. For integers $a, b, b>0$, let us denote by $(a, b)_*$ the greatest divisor of a which is a unitary divisor of b; in case $(a, b)_*=1$, a will be said to be *semiprime* to b. If a and b are positive, $a\neq b$, then the pair $\{a, b\}$ will be termed *co-semiprime*, provided that the smaller of the pair is semiprime to the other. The pair $\{b, b\}$ will be considered a co-semiprime pair only in case $b=1$.

The principal aim of this paper is to illustrate a method in asymptotic number theory whose basic feature is the unitary convolution. This method will be applied to the following questions: (A) the density δ_2 of the set S_2 of the ordered pairs of co-semiprime integers, (B) the average order of the *core* $\gamma(n)$ of n (the maximal square-free divisor of n), (C) the distribution of the *exponentially odd* integers, that is, integers in whose canonical prime-power factorization (3.5) all occurring exponents are odd. We present now a brief survey of the paper.

In § 2 we introduce and evaluate "unitary" analogues of some of the basic arithmetical functions. Corresponding to the Euler φ-function, the *unitary totient* $\varphi^*(n)$ is defined to be the number of integers contained in a residue system (mod n) and semiprime to n. We obtain in (2.8) a simple representation of $\varphi^*(n)$ as a unitary convolution. This result is analogous to the familiar Dedekind-Liouville evaluation of $\varphi(n)$,

$$\varphi(n)=\sum_{d\delta=n}\mu(d)\,\delta, \tag{1.2}$$

where $\mu(n)$ denotes the Möbius function. In our discussion of $\varphi^*(n)$ in § 2, the above definition is replaced by an equivalent definition which makes

possible a simultaneous treatment of $\varphi^*(n)$ and the unitary analogue $\mu^*(n)$ of $\mu(n)$. This is accomplished by introducing a trigonometric sum $c^*(m, n)$ for the case of unitary divisors, corresponding to RAMANUJAN'S sum $c(m, n)$ in the ordinary case. A unitary analogue of the Möbius inversion formula is also proved (Theorem 2.3).

Section 3 is concerned with preliminaries to the asymptotic considerations of the remaining sections. In § 4 we obtain an estimate (Theorem 4.1) for the average order of $f(n)$ as defined by (1.1), with $h(n)=n$ and $g(n)$ bounded. The cases $g(n)=1$ and $g(n)=\mu^*(n)$, respectively, yield results for the sum $\sigma^*(n)$ of the unitary divisors of n (Corollary 4.1) and for $\varphi^*(n)$, (Corollary 4.2). Application is made in Theorem 4.2 to the distribution of the set S_2 defined above. In particular, S_2 is shown to have density α (Corollary 4.2.1), where α is defined by (3.11). Since the subset T_2 of *relatively* prime (co-prime) pairs has density $6/\pi^2$ [*6*, Theorem 332], it must follow that $6/\pi^2 \leqq \delta_2 \leqq 1$. Actually, on the basis of Lemma 3.6, we have $6/\pi^2 < \delta_2 < 1$, which shows that the set S_2 is substantially larger than T_2.

In § 5 we consider the average order of $f(n)$ with $h(n)=\mu^2(n)n$ and $g(n)$ bounded (Theorem 5.1). In the case $g(n)=1$, this theorem reduces to a result for the sum $\sigma'(n)$ of the unitary, square-free divisors of n (Corollary 5.1.1), while in case $g(n)=\mu(n)$, it yields a result for the function $\mu^2(n)\varphi(n)$, (Corollary 5.1.2). The latter result leads to an estimate for the average of the function $\gamma(n)$, (Theorem 5.2). This estimate is an improvement on an earlier approximation proved by WIGERT using analytical methods [*9*].

In § 6 we consider the set Q^* of the exponentially odd numbers defined above. The principal result concerning the distribution of Q^* is contained in Theorem 6.1. We point out the occurrence of the constant α in this result as in the results obtained previously for S_2 and $\gamma(n)$.

While the unitary convolution method appears limited in scope, it is noteworthy that the techniques involved in its application in this paper are elementary in the strictest possible sense. In particular, it is nowhere necessary to introduce generating functions for those arithmetical functions which enter into the discussion.

HISTORICAL REMARK. The function $\varphi^*(n)$ occurs as a particular case of a more general function discussed briefly by DIRICHLET [*4*, § 11], [*3*, p. 122] and later by LERCH [*7*], [*3*, p. 136]. In addition, the function $\sigma^*(n)$ was touched upon by FEKETE [*5*], [*3*, p. 321]. However, the intrinsic interest of these functions seems not to have been recognized by earlier writers. For a discussion of the formal properties of the unitary convolution (1.1), we refer to VAIDYANATHASWAMY [*8*, § II, 6].

2. UNITARY ANALOGUES OF THE ELEMENTARY FUNCTIONS. The set T of integers semiprime to n and contained in a residue system $S \pmod n$ will be designated the *semi-reduced residue system* $\pmod n$ *contained in* S. If S consists of the integers $1, \ldots, n$, then T will be called a *least positive*,

semireduced residue system (mod n). It will be noted that any positive integer $a \leqq n$ can be represented *uniquely* in the form $a = dx$, where d is a unitary divisor of n and x is contained in a least positive, semi-reduced residue system (mod n/d); in fact, $d = (a, n)_*$. This observation can be restated as the enumerative principle:

LEMMA 2.1. *The integers dx, where d ranges over the unitary divisors of n, and for each d, x ranges over a semi-reduced residue system* (mod n/d), *constitute a residue system* (mod n).

With $e(m, n) = \exp(2\pi i m/n)$, we define for arbitrary integers m,

$$c^*(m, n) = \sum_{(x,n)_*=1} e(mx, n), \tag{2.1}$$

the summation extending over the integers x of a semi-reduced residue system (mod n). Obviously, $c^*(m, n)$ is independent of the residue system in the summation.

It is evident that if x ranges over a semi-reduced residue system (mod n) and $(a, n) = 1$, *then ax also ranges over a semi-reduced residue system* (mod n). Hence

LEMMA 2.2. *If $(a, n) = 1$, then $c^*(am, n) = c^*(m, n)$.*

We prove first

THEOREM 2.1.

$$\sum_{\substack{d\delta=n \\ (d,\delta)=1}} c^*(m, d) = \varepsilon(m, n) \equiv \begin{cases} n & (n \mid m) \\ 0 & (n \nmid m). \end{cases} \tag{2.2}$$

PROOF. It is a familiar fact that

$$\eta(m, n) \equiv \sum_{a \,(\mathrm{mod}\, n)} e(ma, n) = \varepsilon(m, n).$$

But by Lemma 2.1, we have

$$\eta(m, n) = \sum_{\substack{d\delta=n \\ (d,\delta)=1}} \sum_{(x,\delta)_*=1} e(mdx, n) = \sum_{\substack{d\delta=n \\ (d,\delta)=1}} c^*(m, \delta).$$

Combining these two relations, (2.2) results.

Define now

$$\varphi^*(n) = c^*(0, n), \qquad \mu^*(n) = c^*(1, n); \tag{2.3}$$

the definition of $\varphi^*(n)$ in (2.3) is evidently equivalent to that given in the Introduction. We thus have the corollaries,

Corollary 2.1.1 ($m = 0$).

$$\sum_{\substack{d\delta=n \\ (d,\delta)=1}} \varphi^*(d) = n; \tag{2.4}$$

Corollary 2.1.2 ($m=1$).

$$\sum_{\substack{d\,\delta=n\\(d,\,\delta)=1}} \mu^*(d) = \varepsilon(n) \equiv \begin{cases} 1 & (n=1) \\ 0 & (n>1). \end{cases} \tag{2.5}$$

Next we prove

THEOREM 2.2. *The function $c^*(m, n)$ is multiplicative as a function of n; that is, $c^*(m, 1)=1$, and if $n=n_1 n_2$, $(n_1, n_2)=1$, then $c^*(m, n)=c^*(m, n_1)\, c^*(m, n_2)$.*

PROOF. If x_1 and x_2 range over residue systems (mod n_1) and (mod n_2) respectively, then $x_2 n_1 + x_1 n_2$ ranges over a residue system (mod $n_1 n_2$). If $(x_2 n_1 + x_1 n_2, n)_* = 1$, then since $(n_1, n_2)=1$, it must follow that $(x_1, n_1)_* = (x_2, n_2)_* = 1$. Conversely, if either $(x_1, n_1)_*$ or $(x_2, n_2)_*$ is $\neq 1$, then $(x_2 n_1 + x_1 n_2, n)_* \neq 1$. Hence the set $\{x_2 n_1 + x_1 n_2\}$ yields a semi-reduced residue system (mod n) if x_1 and x_2 range over semi-reduced residue systems (mod n_1) and (mod n_2), respectively.

Therefore, by (2.1) one obtains, on placing $x = x_2 n_1 + x_1 n_2$, and using the additivity of $e(m, n)$,

$$c^*(m, n) = \sum_{\substack{(x_1, n_1)_*=1\\(x_2, n_2)_*=1}} e\big(m(x_2 n_1 + x_1 n_2), n\big) = c^*(m n_1, n_2)\, c^*(m n_2, n_1),$$

and the Theorem follows by Lemma 2.2.

COROLLARY 2.2.1 ($m=0$). *The function $\varphi^*(n)$ is multiplicative.*

COROLLARY 2.2.2 ($m=1$). *The function $\mu^*(n)$ is multiplicative.*

An important and simple consequence of the property (2.5) of $\mu^*(n)$ is the following analogue of the Möbius inversion formula.

THEOREM 2.3. *For arithmetical functions $f_1(n)$, $f_2(n)$,*

$$f_1(n) = \sum_{\substack{d\,\delta=n\\(d,\,\delta)=1}} f_2(d) \rightleftharpoons f_2(n) = \sum_{\substack{d\,\delta=n\\(d,\,\delta)=1}} \mu^*(d)\, f_1(\delta); \tag{2.6}$$

in particular, every arithmetical function $f_1(n)$ has a unique representation of the form $\Sigma_d f_2(d)$, where the summation is over the unitary divisors d of n.

PROOF. Suppose $f_2(n)$ to be defined as on the right of (2.6). Then

$$S \equiv \sum_{\substack{d\,\delta=n\\(d,\,\delta)=1}} f_2(d) = \sum_{\substack{d\,\delta=n\\(d,\,\delta)=1}} \sum_{\substack{D\,E=d\\(D,\,E)=1}} \mu^*(D)\, f_1(E) = \sum_{E\mid n} f_1(E) \sum_{\substack{D\,\delta=\frac{n}{E}\\(D\,E,\,\delta)=1\\(D,\,E)=1}} \mu^*(D)$$

$$= \sum_{\substack{E\mid n\\(E,\,\frac{n}{E})=1}} f_1(E) \sum_{\substack{D\,\delta=\frac{n}{E}\\(D,\,\delta)=1}} \mu^*(D),$$

so that $S=f_1(n)$, by Corollary 2.1.2. The converse can be similarly proved.

As a consequence of Theorem 2.3 and (2.2), the following evaluation of $c^*(m, n)$ results.

THEOREM 2.4.

$$c^*(m,n)=\sum_{\substack{d\delta=n\\(d,\delta)=1,\ \delta\mid m}}\mu^*(d)\,\delta. \tag{2.7}$$

COROLLARY 2.4.1 $(m=0)$.

$$\varphi^*(n)=\sum_{\substack{d\delta=n\\(d,\delta)=1}}\mu^*(d)\,\delta. \tag{2.8}$$

Finally, we deduce an explicit evaluation of $\mu^*(n)$. For this purpose, let $\omega(n)$ denote the number of distinct prime divisors of n, $\omega(1)=0$.

THEOREM 2.5.

$$\mu^*(n)=(-1)^{\omega(n)}; \tag{2.9}$$

that is, $\mu^*(n)$ is $+1$ or -1 according as n has an even or an odd number of distinct prime divisors.

PROOF. If suffices, by virtue of the multiplicative property of $\mu^*(n)$ proved in Corollary 2.2.2, to verify (2.9) in the case $n=p^k$, p prime. But by (2.5), $\mu^*(1)=1$, and if $k>0$, $\mu^*(p^k)=-1$. This proves the theorem.

REMARK 2.1. In particular, $\mu^*(n)$ is bounded.

3. BACKGROUND. This section consists of a number of lemmas which will be referred to repeatedly in the later sections. In the remainder of the paper x will denote a real variable, usually $\geqq 1$. Let $\tau(n)$ denote the number of divisors of n. The following estimates are well known [6, §§ 18, 18.2].

LEMMA 3.1. *For all $\varepsilon>0$, $x\geqq 2$,*

$$\tau(n)=O(n^{\varepsilon}); \tag{3.1}$$

$$T(x)\equiv\sum_{n\leqq x}\tau(n)=O(x\log x). \tag{3.2}$$

Define now $q(n)$ to be 1 or 0 according as n is or is not square-free, and place $\mu_2(n)=\mu(m)$ if $n=m^2$ is a square, $=0$ otherwise.

LEMMA 3.2.

$$q(n)=\sum_{d\mid n}\mu_2(d); \tag{3.3}$$

$$Q(x)\equiv\sum_{n\leqq x}q(n)=\frac{6x}{\pi^2}+O(\sqrt{x}). \tag{3.4}$$

These are the classical elementary results concerned with the distribution of the square-free numbers [6, § 18.6].

Suppose now that n possesses k distinct prime factors, $p_1,\ldots,p_k$, and place

$$n=p_1^{t_1}\ldots p_k^{t_k}. \tag{3.5}$$

Further, let $J(n)$ denote the Jordan totient of second order [3, p. 147].

LEMMA 3.3. *If n is defined by* (3.5), *then*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \quad J(n) = n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right); \tag{3.6}$$

moreover, for every $\varepsilon > 0$,

$$\frac{J(n)}{n^{2-\varepsilon}} \to \infty \quad as \quad n \to \infty. \tag{3.7}$$

The result in (3.7) is the case $s = 2$ of [2, Lemma 12]; it can be proved in the same way as the corresponding result for $\varphi(n)$, [6, Theorem 327]. The other statements of Lemma 3.3 are well known. Generalizing (1.2), the Legendre totient $\varphi(x, n)$, defined to be the number of integers $\leqq x$ which are prime to n, has the evaluation [3, p. 115],

$$\varphi(x, n) = \sum_{d|n} \mu(d) \left[\frac{x}{d}\right]. \tag{3.8}$$

We use this fact to prove the following useful result. Let $\vartheta(n)$ denote the number of square-free divisors of n; then

LEMMA 3.4.

$$\varphi(x, n) = \frac{x\varphi(n)}{n} + O\left(\vartheta(n)\right), \tag{3.9}$$

uniformly in x.

REMARK 3.1. In computations it is sometimes convenient to replace $\vartheta(n)$ by the more familiar function $\tau(n)$; obviously, $\vartheta(n) \leqq \tau(n)$.

PROOF. By (3.8) and the boundedness of $\mu(n)$,

$$\varphi(x, n) = \sum_{d|n} \mu(d) \left(\frac{x}{d} + O(1)\right) = x \sum_{d|n} \frac{\mu(d)}{d} + O\left(\vartheta(n)\right),$$

and (3.9) follows on the basis of (1.2).

The remaining lemmas are concerned with the constant α mentioned in the Introduction.

LEMMA 3.5. *The series,*

$$\sum_{n=1}^{\infty} \frac{\mu^*(n)\varphi(n)}{n^3}, \qquad \sum_{n=1}^{\infty} \frac{\mu(n)\varphi(n)}{nJ(n)} \tag{3.10}$$

converge absolutely; denoting their sums by S and S' respectively,

$$S = S' = \alpha \equiv \prod_{p} \left(1 - \frac{1}{p(p+1)}\right) \tag{3.11}$$

where the product is extended over the primes.

PROOF. The first series in (3.10) converges absolutely, because $\mu^*(n)$ is bounded (Remark 2.1) and $\varphi(n) \leqq n$. The absolute convergence of the second series is a consequence of (3.7). Since the general terms of both series are multiplicative as functions of n, they may be expanded into infinite products of Euler type [6, § 17.4]. In particular, by (3.6)

$$S = \sum_{n=1}^{\infty} \frac{\mu^*(n)\,\varphi(n)}{n^3} = \prod_p \left(\sum_{k=1}^{\infty} \frac{\mu^*(p^k)\,\varphi(p^k)}{p^{3k}} \right) = \prod_p \left\{ 1 - \left(\frac{p-1}{p} \right) \sum_{k=1}^{\infty} \left(\frac{1}{p^2} \right)^k \right\}$$

$$= \prod_p \left(1 - \frac{1}{p^2 + p} \right).$$

A similar product expansion is obtained for S', thereby proving the Lemma.

Let $\zeta(s)$ denote the Riemann ζ-function, $s > 1$.

LEMMA 3.6. *If α is defined by* (3.11), *then*

$$6/\pi^2 < \alpha < 1. \tag{3.12}$$

PROOF. By (3.11) and the fact that $\zeta(2) = \prod \left(1 - \frac{1}{p^2} \right)^{-1} = \frac{6}{\pi^2}$.

4. THE CASE $h(n) = n$ AND PROBLEM A. We prove first

LEMMA 4.1.

$$\varphi_1(x, n) \equiv \sum_{\substack{m \leqq x \\ (m,n)=1}} m = \frac{x^2\,\varphi(n)}{2n} + O\left(x\,\vartheta(n)\right). \tag{4.1}$$

PROOF. By partial summation and the definition of $\varepsilon(n)$, (2.5),

$$\begin{aligned} \varphi_1(x, n) &= \sum_{m \leqq x} m\,\varepsilon\left((m, n)\right) = -\sum_{m \leqq x} \sum_{a \leqq m} \varepsilon\left((a, n)\right) + \sum_{m \leqq x} \varepsilon\left((m, n)\right)([x] + 1) \\ &= -\sum_{m \leqq x} \varphi(m, n) + ([x] + 1)\,\varphi(x, n) \equiv \Sigma_1 + \Sigma_2; \end{aligned} \tag{4.2}$$

let us say. Appealing to (3.9), one obtains

$$\begin{aligned} \Sigma_1 &\equiv -\sum_{m \leqq x} \varphi(m, n) = -\sum_{m \leqq x} \left(\frac{m\,\varphi(n)}{n} + O\left(\vartheta(n)\right) \right) \\ &= -\frac{\varphi(n)}{n} \sum_{m \leqq x} m + O\left(x\,\vartheta(n)\right) = -\frac{\varphi(n)}{n} \left(\frac{x^2}{2} + O(x) \right) + O\left(x\,\vartheta(n)\right); \end{aligned}$$

therefore, since $\varphi(n) \leqq n$, $\vartheta(n) \geqq 1$, one deduces

$$\Sigma_1 = -\frac{\varphi(n)\,x^2}{2n} + O\left(x\,\vartheta(n)\right). \tag{4.3}$$

Also,

$$\Sigma_2 \equiv ([x] + 1)\,\varphi(x, n) = x\,\varphi(x, n) + O\left(\varphi(x, n)\right) = x\,\varphi(x, n) + O(x),$$

so that by Lemma 3.4,

$$\Sigma_2 = \frac{\varphi(n)\, x^2}{n} + O\left(x\, \vartheta(n)\right). \tag{4.4}$$

The Lemma results on collecting (4.2), (4.3), and (4.4).

We now prove the first main result of this section. For this purpose, place $h(n) = n$ in (1.1) so that

$$f(n) = \sum_{\substack{d\,\delta = n \\ (d,\,\delta)=1}} g(d)\, \delta. \tag{4.5}$$

THEOREM 4.1. *If $f(n)$ is defined by (4.5) and $g(n)$ is bounded, then for $x \geqq 2$,*

$$\sum_{n \leqq x} f(n) = \frac{x^2}{2} \sum_{n=1}^{\infty} \frac{g(n)\, \varphi(n)}{n^3} + O\left(x \log^2 x\right). \tag{4.6}$$

REMARK 4.1. The series is absolutely convergent because $g(n)\, \varphi(n) = O(n)$.

PROOF. By (4.5),

$$\sum_{n \leqq x} f(n) = \sum_{\substack{d\,\delta \leqq x \\ (d,\,\delta)=1}} g(d)\, \delta = \sum_{d \leqq x} g(d)\, \varphi_1\left(\frac{x}{d},\, d\right);$$

hence, applying Lemma 4.1 and Remark 3.1, it follows, since $g(n)$ is bounded, that

$$\sum_{n \leqq x} f(n) = \frac{x^2}{2} \sum_{d \leqq x} \frac{g(d)\, \varphi(d)}{d^3} + O\left(x \sum_{d \leqq x} \frac{\tau(d)}{d}\right).$$

Now

$$\sum_{n \leqq x} \frac{\tau(n)}{n} = \sum_{d\,\delta \leqq x} \frac{1}{d\,\delta} \leqq \left(\sum_{m \leqq x} \frac{1}{m}\right)^2 = O\left(\log^2 x\right),$$

a fact which also may be deduced from (3.2). Thus

$$\sum_{n \leqq x} f(n) = \frac{x^2}{2} \sum_{n=1}^{\infty} \frac{g(n)\, \varphi(n)}{n^3} + O\left(x^2 \sum_{n > x} \frac{\varphi(n)}{n^3}\right) + O\left(x \log^2 x\right).$$

However,

$$\sum_{n > x} \frac{\varphi(n)}{n^3} = O\left(\sum_{n > x} \frac{1}{n^2}\right) = O\left(\frac{1}{x}\right),$$

and the Theorem results immediately.

We note the corollaries corresponding to the cases $g(n) = 1$ and $g(n) = \mu^*(n)$. By [6, Theorem 288].

COROLLARY 4.1.1 $\left(g(n) = 1\right)$. *If $x \geqq 2$, then*

$$\sum_{n \leqq x} \sigma^*(n) = \frac{\pi^2 x^2}{12\, \zeta(3)} + O\left(x \log^2 x\right). \tag{4.7}$$

Also, on the basis of (2.8) and Lemma 3.5, one obtains

COROLLARY 4.1.2 $(g(n)=\mu^*(n))$. *If* $x\geqq 2$, *then*

$$\Phi^*(x) \equiv \sum_{n\leqq x} \varphi^*(n) = \frac{\alpha x^2}{2} + O(x\log^2 x), \tag{4.8}$$

where α *is defined by* (3.11).

The result in (4.8) furnishes a means for solving Problem *A*. Let $S_2(x)$ denote the number of pairs $\{a, b\}$ with $1\leqq a\leqq x$, $1\leqq b\leqq x$ contained in S_2. With $\Phi^*(x)$ denoting the summatory function of $\varphi^*(n)$, we have

LEMMA 4.2.

$$S_2(x) = 2\Phi^*(x) - 1. \tag{4.9}$$

PROOF. For each b, $1\leqq b\leqq x$, choose all pairs $\{a, b\}$ such that a is contained in a least positive, semi-reduced residue system (mod b). The number of such pairs is $\Phi^*(x)$. Repeating this process with the rôles of a and b interchanged, one obtains in toto $2\Phi^*(x)$ co-semiprime pairs $\{a, b\}$ satisfying $1\leqq a\leqq x$, $1\leqq b\leqq x$, with the sole duplication of the pair $\{1, 1\}$. This establishes the Lemma.

THEOREM 4.2. *For* $x\geqq 2$,

$$S_2(x) = \alpha x^2 + O(x\log^2 x). \tag{4.10}$$

PROOF. The result is an immediate result of Lemma 4.2 and Corollary 4.1.2.

COROLLARY 4.2.1. *The set* S_2 *has asymptotic density* α; *that is*

$$\lim_{x\to\infty} \frac{S_2(x)}{x^2} = \alpha. \tag{4.11}$$

5. THE CASE $h(n)=\mu^2(n)n$ AND PROBLEM B. The following lemma can be easily proved in the manner of [*I*, (5.2), $k=1$, $s=2$] and is in fact a consequence of that result by Dirichlet multiplication.

LEMMA 5.1.

$$\zeta_n^* \equiv \sum_{\substack{m=1\\(m,n)=1}}^{\infty} \frac{\mu(m)}{m^2} = \frac{n^2}{\zeta(2)J(n)}. \tag{5.1}$$

The next result generalizes (3.4), $(n=1)$.

LEMMA 5.2.

$$Q_n(x) \equiv \sum_{\substack{m\leqq x\\(m,n)=1}} \mu^2(m) = \beta(n)x + O\left(\sqrt{x}\,\vartheta(n)\right), \tag{5.2}$$

where $\beta(n) = n\varphi(n)/\zeta(2)J(n)$.

REMARK 5.1. It is noted by (3.6) that $\beta(n) \leqq 1$.

PROOF. Let $q_n(m)$ be defined to be 1 if m is square-free and $(m, n) = 1$, and 0 otherwise. By (3.3) we have

$$q_n(m) = \varepsilon\big((m, n)\big)\, q(m) = \varepsilon\big((m, n)\big) \sum_{d^2 \delta = m} \mu(d).$$

Hence

$$Q_n(x) = \sum_{m \leqq x} q_n(m) = \sum_{\substack{d^2 \delta \leqq x \\ (d, n) = (\delta, n) = 1}} \mu(d) = \sum_{\substack{d \leqq \sqrt{x} \\ (d, n) = 1}} \mu(d)\, \varphi\left(\frac{x}{d^2}, n\right).$$

Application of Lemma 3.4 yields, by definition of ζ_n^*,

$$\begin{aligned} Q_n(x) &= \frac{x\varphi(n)}{n} \sum_{\substack{d \leqq \sqrt{x} \\ (d, n) = 1}} \frac{\mu(d)}{d^2} + O\left(\sum_{\substack{d \leqq \sqrt{x} \\ (d, n) = 1}} \vartheta(n) \right) \\ &= \frac{x\varphi(n)}{n} \frac{\zeta_n^*}{} + O\left(\frac{x\varphi(n)}{n} \sum_{d > \sqrt{x}} \frac{1}{d^2} \right) + O\big(\vartheta(n)\, \varphi(\sqrt{x}, n)\big) \\ &= \frac{x\varphi(n)}{n} \frac{\zeta_n^*}{} + O\left(\frac{\sqrt{x}\, \varphi(n)}{n} \right) + O\big(\sqrt{x}\, \vartheta(n)\big), \end{aligned}$$

and Lemma 5.2 results by virtue of (5.1).

LEMMA 5.3.

$$Q_n'(x) \equiv \sum_{\substack{m \leqq x \\ (m, n) = 1}} \mu^2(m)\, m = \frac{\beta(n)\, x^2}{2} + O\big(x^{\frac{3}{2}} \vartheta(n)\big), \tag{5.3}$$

where $\beta(n)$ is defined as in the preceding lemma.

PROOF. Using the notation introduced in Lemma 5.2, it follows by partial summation that

$$Q_n'(x) = \sum_{m \leqq x} q_n(m)\, m \equiv \Sigma_1 + \Sigma_2, \tag{5.4}$$

where

$$\Sigma_1 = -\sum_{m \leqq x} Q_n(m), \qquad \Sigma_2 = Q_n(x)\,([x] + 1).$$

By Lemma 5.2,

$$\begin{aligned} \Sigma_1 &= -\beta(n) \sum_{m \leqq x} m + O\Big(\vartheta(n) \sum_{m \leqq x} m^{\frac{1}{2}}\Big) \\ &= -\beta(n)\left(\frac{x^2}{2} + O(x)\right) + O\big(\vartheta(n)\, x^{\frac{3}{2}}\big), \end{aligned}$$

so that by Remark 5.1,

$$\Sigma_1 = -\frac{\beta(n)\, x^2}{2} + O\big(x^{\frac{3}{2}} \vartheta(n)\big). \tag{5.5}$$

Since for all n, $Q_n(x) \leqq Q_1(x) = Q(x)$, it follows by Lemma 3.2 that

$$\Sigma_2 = Q_n(x)\,(x + O(1)) = x\,Q_n(x) + O\,(Q(x)) = x\,Q_n(x) + O(x),$$

and therefore by (5.2),

$$\Sigma_2 = \beta(n)\,x^2 + O\left(x^{\frac{3}{2}}\,\vartheta(n)\right). \tag{5.6}$$

The Lemma follows, by (5.4), (5.5), and (5.6).

The following lemma will be needed for the second corollary to the next theorem.

LEMMA 5.4.

$$\varphi'(n) \equiv \mu^2(n)\,\varphi(n) = \sum_{\substack{d\,\delta = n \\ (d,\,\delta)=1}} \mu(d)\,\mu^2(\delta)\,\delta. \tag{5.7}$$

PROOF. By (1.2) and the multiplicativity of $\mu(n)$,

$$\varphi'(n) = \sum_{d\,\delta = n} \mu^2(d\,\delta)\,\mu(d)\,\delta = \sum_{\substack{d\,\delta = n \\ (d,\,\delta)=1}} \mu^2(d)\,\mu(d)\,\mu^2(\delta)\,\delta,$$

from which (5.7) results.

In this section we consider (1.1) in the case $h(n) = \mu^2(n)\,n$, that is,

$$f(n) = \sum_{\substack{d\,\delta = n \\ (d,\,\delta)=1}} g(d)\,\mu^2(\delta)\,\delta. \tag{5.8}$$

THEOREM 5.1. *If $g(n)$ is bounded and $f(n)$ is defined by* (5.8), *then*

$$\sum_{n \leqq x} f(n) = \frac{x^2}{2\,\zeta(2)} \sum_{n=1}^{\infty} \frac{g(n)\,\varphi(n)}{n\,J(n)} + O(x^{\frac{3}{2}}). \tag{5.9}$$

REMARK 5.2. The series is absolutely convergent, by the same argument used in the case $g(n) = \mu(n)$ considered in Lemma 3.5.

PROOF. By (5.8) and the definition of $Q'_n(x)$ in (5.3)

$$\sum_{n \leqq x} f(n) = \sum_{\substack{d\,\delta \leqq x \\ (d,\,\delta)=1}} g(d)\,\mu^2(\delta)\,\delta = \sum_{d \leqq x} g(d)\,Q'_d\left(\frac{x}{d}\right),$$

so that by Lemma 5.3, Remark 3.1, and the boundedness of $g(n)$,

$$\sum_{n \leqq x} f(n) = \frac{x^2}{2} \sum_{d \leqq x} \frac{g(d)\,\beta(d)}{d^2} + \left(x^{\frac{3}{2}} \sum_{d \leqq x} \frac{\tau(d)}{d^{\frac{3}{2}}}\right).$$

On the basis of (3.1) and Remark 5.1, it therefore follows that

$$\sum_{n \leqq x} f(n) = \frac{x^2}{2} \sum_{n=1}^{\infty} \frac{g(n)\,\beta(n)}{n^2} + O\left(x^2 \sum_{n > x} \frac{1}{n^2}\right) + O(x^{\frac{3}{2}}),$$

and the Theorem results by definition of $\beta(n)$, because the first O-term is $O(x)$.

It should be noted that, in case $g(n)=1$, $f(n)$ in (5.8) becomes the function $\sigma'(n)$ mentioned in § 1. Hence

COROLLARY 5.1.1. $(g(n)=1)$.

$$\sum_{n\leqq x}\sigma'(n)=\frac{\alpha' x^2}{2}+O(x^{\frac{3}{2}}), \tag{5.10}$$

where

$$\alpha'\equiv\zeta^{-1}(2)\sum_{n=1}^{\infty}\frac{\varphi(n)}{n\,f(n)}=\prod_{p}\left(1-\frac{1}{p^2}+\frac{1}{p(p+1)}\right).$$

The product expansion of α' is deduced in the same manner as the expansions of Lemma 3.5.

The case $g(n)=\mu(n)$ in (5.8) yields the function $\varphi'(n)$ in (5.7). Thus by Lemma 3.5,

COROLLARY 5.1.2 $(g(n)=\mu(n))$.

$$\Phi'(x)\equiv\sum_{n\leqq x}\varphi'(n)=\frac{\alpha x^2}{2\zeta(2)}+O(x^{\frac{3}{2}}). \tag{5.11}$$

We now turn to Problem B. Let $\gamma(n)$ be defined as in the Introduction.

LEMMA 5.5 (cf. WIGERT [9, (3)]).

$$\gamma(n)=\sum_{d|n}\varphi'(d),\qquad \varphi'(n)=\mu^2(n)\,\varphi(n). \tag{5.12}$$

PROOF. Möbius inversion applied to (1.2) yields the familiar formula of GAUSS, $n=\sum_{d|n}\varphi(d)$; replacing n by $\gamma(n)$ in this relation, one obtains

$$\gamma(n)=\sum_{d|\gamma(n)}\varphi(d)=\sum_{\substack{d|n\\ (d\text{ square-free})}}\varphi(d),$$

which is the same as (5.12).

THEOREM 5.2.

$$\sum_{n\leqq x}\gamma(n)=\frac{\alpha x^2}{2}+O(x^{\frac{3}{2}}), \tag{5.13}$$

where α is defined by (3.11).

PROOF. By (5.12) and the definition of $\Phi'(x)$ in (5.11)

$$\sum_{n\leqq x}\gamma(n)=\sum_{d\,\delta\leqq x}\varphi'(d)=\sum_{n\leqq x}\Phi'\left(\frac{x}{n}\right);$$

thus application of Corollary 5.1.2 leads to

$$\begin{aligned}\sum_{n\leqq x}\gamma(n)&=\frac{\alpha x^2}{2\zeta(2)}\sum_{n\leqq x}\frac{1}{n^2}+O\left(x^{\frac{3}{2}}\sum_{n\leqq x}\frac{1}{n^{\frac{3}{2}}}\right)\\&=\frac{\alpha x^2}{2}+O\left(x^2\sum_{n>x}\frac{1}{n^2}\right)+O(x^{\frac{3}{2}})=\frac{\alpha x^2}{2}+O(x^{\frac{3}{2}}).\end{aligned}$$

The Theorem is proved.

Finally, we remark that (5.11) and (5.13) improve estimates of WIGERT involving remainder terms of order $x^{\frac{1}{2}}$ [9, (5), (6)]. Contrary to the approach of this paper, WIGERT obtained independently his estimate for the average of $\gamma(n)$ and from that result deduced an estimate for $\Phi'(x)$.

6. PROBLEM C. Preparatory to the main discussion we prove

LEMMA 6.1. *If $g(n)$ and $h(n)$ are multiplicative functions, then the unitary convolution (1.1) of $g(n)$ and $h(n)$ is also multiplicative.*

PROOF. Certainly $f(1)=1$ if $g(1)=h(1)=1$. Suppose then that $n=n_1 n_2$, $(n_1, n_2)=1$. If $n=d\delta$, then d and δ have *unique* factorizations, $d=d_1 d_2$, $\delta=\delta_1 \delta_2$, such that $n_1=d_1\delta_1$, $n_2=d_2, \delta_2$. Moreover, $(d, \delta)=1 \rightleftharpoons (d_1, \delta_1)=(d_2, \delta_2)=1$. Hence

$$f(n)=\sum_{\substack{d_1\delta_1=n_1\\ d_2\delta_2=n_2\\ (d_1,\delta_1)=(d_2,\delta_2)=1}} f(d_1 d_2)\, g(\delta_1\delta_2)=\sum_{\substack{d_1\delta_1=n_1\\ (d_1,\delta_1)=1}} f(d_1)\, g(\delta_1)\sum_{\substack{d_2\delta_2=n_2\\ (d_2,\delta_2)=1}} f(d_2)\, g(\delta_2),$$

and the Lemma is proved.

Let $q^*(n)$ denote the characteristic function of Q^*, that is, $q^*(n)=1$ or 0 according as n is or is not exponentially odd. It will be observed that $n\in Q^*$ if and only if its greatest unitary, square divisor is 1. Thus, the exponentially odd numbers may be viewed as "unitary" analogues of the square-free numbers. Pursuing this analogy [cf. (3.3)], we define $\mu_2^*(n)$ by the relation,

$$\sum_{\substack{d\delta=n\\ (d,\delta)=1}} \mu_2^*(d)=q^*(n). \tag{6.1}$$

Certainly, (6.1) defines $\mu_2^*(n)$ uniquely, in view of Theorem 2.3. In fact we have the following evaluation.

LEMMA 6.2.

$$\mu_2^*(n)=\begin{cases}\mu^*(\sqrt{n}) & \textit{if } n \textit{ is a square.}\\ 0 & \textit{otherwise.}\end{cases} \tag{6.2}$$

PROOF. On the basis of (2.6) and (6.1)

$$\mu_2^*(n)=\sum_{\substack{d\delta=n\\ (d,\delta)=1}} \mu^*(d)\, q^*(\delta). \tag{6.3}$$

It is easily seen that $q^*(n)$ is multiplicative, and hence also $\mu_2^*(n)$, by Corollary 2.2.2, Lemma 6.1, and (6.3). It therefore suffices to evaluate $\mu_2^*(n)$ for $n=p^k$, p prime. But by (6.3), $\mu_2^*(p^k)=0$ or -1 according as k is odd or $k\neq 0$ is even. This completes the proof.

LEMMA 6.3.

$$\varphi(n^2)=n\,\varphi(n). \tag{6.4}$$

PROOF. By (1.2),

$$\varphi(n^2) = \sum_{d|n^2} \left(\frac{n^2}{d}\right) \mu(d) = n \sum_{d|n} \left(\frac{n}{d}\right) \mu(d) = n\,\varphi(n).$$

LEMMA 6.4.

$$\vartheta(n^2) = \vartheta(n). \tag{6.5}$$

We are now in a position to prove

THEOREM 6.1. *If* $x \geqq 2$, *then*

$$Q^*(x) \equiv \sum_{n \leqq x} q^*(n) = \alpha\, x + O(\sqrt{x} \log x), \tag{6.6}$$

where α *is defined by* (3.11).

PROOF. On the basis of (6.1) one obtains

$$Q^*(x) = \sum_{\substack{d\,\delta \leqq x \\ (d,\,\delta)=1}} \mu_2^*(d) = \sum_{d \leqq x} \mu_2^*(d)\, \varphi\left(\frac{x}{d}, d\right),$$

so that by Lemma 6.2,

$$Q^*(x) = \sum_{n \leqq \sqrt{x}} \mu^*(n)\, \varphi\left(\frac{x}{n^2}, n^2\right). \tag{6.7}$$

Hence by Lemmas 3.4, 6.3, and 6.4, and Remark 2.1,

$$\begin{aligned} Q^*(x) &= x \sum_{n \leqq \sqrt{x}} \frac{\mu^*(n)\,\varphi(n^2)}{n^4} + O\Big(\sum_{n \leqq \sqrt{x}} \vartheta(n^2)\Big) \\ &= x \sum_{n \leqq \sqrt{x}} \frac{\mu^*(n)\,\varphi(n)}{n^3} + O\Big(\sum_{n \leqq \sqrt{x}} \vartheta(n)\Big). \end{aligned}$$

Application of Lemma 3.5 and Remark 3.1 yields, by the boundedness of $\mu^*(n)$,

$$Q^*(x) = \alpha\, x + O\left(x \sum_{n > \sqrt{x}} \frac{1}{n^2}\right) + O\big(T(\sqrt{x})\big). \tag{6.8}$$

Since the first O-term in (6.8) is $O(\sqrt{x})$, the Theorem results on appealing to (3.2).

COROLLARY 6.1.1. *The asymptotic density* $\delta(Q^*)$ *of* Q^* *is* α:

$$\delta(Q^*) \equiv \lim_{x \to \infty} \frac{Q^*(x)}{x} = \alpha. \tag{6.9}$$

We note that $Q < Q^*$ where Q denotes the set of all squarefree numbers. By (3.12), (6.9), and the well-known fact that $\delta(Q) = 6/\pi^2$ [see (3.4)], it follows that $\delta(Q) < \delta(Q^*)$.

REMARK 6.1. In another paper concerned with a generalization of Problem C, it is shown that the remainder term in (6.6) can be refined somewhat but at the expense of introducing generating functions in the proof.

Bibliography

[1] Cohen, E.: An extension of Ramanujan's sum, III. Connections with totient functions. Duke Math. J. **23**, 623—630 (1956). — [2] Cohen, E.: Trigonometric sums in elementary number theory. Amer. Math. Monthly **66**, 105—117 (1959). — [3] Dickson, L. E.: History of the Theory of Numbers, vol. I. New York, reprinted 1952. — [4] Dirichlet, P. G. Lejeune: Vorlesungen über Zahlentheorie, 4th ed. Brunswick 1894 (edited by R. Dedekind). — [5] Fekete, M.: Über die additive Darstellung einiger zahlentheoretischer Funktionen. Math. u. naturwiss. Berichte aus Ungarn **26**, 196—211 (1913). — [6] Hardy, G. H., and E. M. Wright: Introduction to the Theory of Numbers, 3rd ed. Oxford 1954. — [7] Lerch, M.: Démonstration élémentaire d'un théorème d'arithmétique. Sitzungsber. der Böhmischen Ges. Wiss., Prag, No. 2, 1903, 3pp. — [8] Vaidyanathaswamy, R.: The theory of multiplicative arithmetical functions. Trans. Amer. Math. Soc. **33**, 579—662 (1931). — [9] Wigert, S.: Sur quelques formules asymptotiques de la théorie des nombres. Arkiv för Mat. Astr. Fys. **22**, 6 pp. (1932).

Dept. of Math., The University of Tennessee, Knoxville, Tenn. (U.S.A.)

(Eingegangen am 19. Januar 1960)

Krull, W.
Math. Zeitschr. 74, 81—90 (1960)

Über die Endomorphismen von total geordneten Archimedischen Abelschen Gruppen

Herrn Joseph E. Hofmann zum 60. Geburtstag gewidmet

Von

Wolfgang Krull

Im folgenden soll gezeigt werden, daß die Eigenart und Schönheit der Proportionenlehre des Eudoxos, die im 5. Buch von Euklids Elementen dargestellt ist, dem modernen Leser erst dann richtig verständlich wird, wenn er die Theorie des Eudoxos mit der Theorie beliebiger total geordneter Archimedischer Abelscher Gruppen in Zusammenhang bringt. Es wird sich nämlich ergeben, daß die Proportionsdefinition des Eudoxos und die Hauptsätze über Proportionen in der Anordnung, wie sie im 5. Buch Euklids hergeleitet sind, die richtige Grundlage bieten, um sehr rasch die Hauptsätze über die Endomorphismenhalbgruppen der Gruppen unseres Typs herzuleiten, so daß man mit einem gewissen Recht sagen darf, diese Sätze „ständen schon bei Euklid". (Im Sinne der Feststellung „es steht alles bei Dedekind", die Emmy Noether oft bei ihren idealtheoretischen Untersuchungen machte.) Auf Grund der gewonnen Resultate soll dann untersucht werden, ob es nicht auch heute noch durchaus sinnvoll sein kann, die Theorie der Körper von reellen Zahlen nicht auf dem allgemein in der Analysis üblichen Weg, sondern unter stärkerem Anschluß an die Griechen als Automorphismen-Theorie Archimedischer Größensysteme zu entwickeln.

§ 1. Beliebige Abelsche Gruppen

Es sei $\mathfrak{A}$ irgendeine feste Abelsche Gruppe. Unter einem *Endomorphismus* von $\mathfrak{A}$ verstehen wir einen Homomorphismus *von* $\mathfrak{A}$ in $\mathfrak{A}$. Ein *Endo-Isomorphismus* bzw. *Automorphismus* ist ein Isomorphismus von $\mathfrak{A}$ *in* $\mathfrak{A}$ bzw. *auf* $\mathfrak{A}$. Die Multiplikation und die Addition der Endomorphismen sind wie üblich definiert. E ist der identische, N der Null-Endomorphismus. Im übrigen bezeichnen $H, Z, \ldots$ Endomorphismen; $A, B, \ldots$ Automorphismen; $a, b, c, \ldots$ Gruppenelemente; $n, m, \ldots$ ganze Zahlen. Unter einem „Ring" bzw. „Körper" verstehen wir stets einen mit *kommutativer* Multiplikation. Ist die Möglichkeit einer nicht kommutativen Multiplikation zugelassen, so sprechen wir von einem *Schiefring* bzw. *Schiefkörper*. Alle betrachteten Ringe sollen ein Einselement besitzen. — Unseren Ausgangspunkt bildet die triviale Bemerkung:

Hilfssatz 1. *Ist die Gruppe $\mathfrak{A}$ gleichzeitig ein Schiefring mit Einselement e, und definiert man den Endomorphismus H_a $(a \in \mathfrak{A})$ durch „$H_a c = a \cdot c$ für alle $c \in \mathfrak{A}$", so bildet die Menge aller H_a eine Halbgruppe $\mathfrak{E}_e$ mit Einselement E, und es gibt in $\mathfrak{E}_e$ für jedes $a \in \mathfrak{A}$ genau ein H mit $He = a$.*

Der Schiefring $\mathfrak{A}$ ist dann und nur dann ein Ring, wenn $\mathfrak{C}_e$ Abelsch ist.

Wir definieren nun: Eine Endomorphismen-Halbgruppe $\mathfrak{A}$ (mit Einselement E) der Gruppe $\mathfrak{A}$ soll *e-transitiv* bzw. *e-einfach-transitiv* heißen, wenn sie für jedes $a \in \mathfrak{A}$ mindestens ein bzw. genau ein H mit $He = a$ enthält. Unser nächstes Hauptziel ist der Nachweis, daß Hilfssatz 1 gewissermaßen umgekehrt werden kann, wenn wir uns auf die Frage beschränken, auf welche Weise sich eine gegebene Gruppe $\mathfrak{A}$ zum *Ring* machen läßt. Auf die Schwierigkeiten, die auftreten, wenn wir über das Kommutative hinausgehen wollen, wird zum Schluß von § 1 kurz eingegangen.

HILFSSATZ 2. *Es sei $\mathfrak{A}$ eine e-einfach-transitive Abelsche Endomorphismen-Halbgruppe. Dann gilt:*

a) *Gibt es zu $e' \in \mathfrak{A}$ in $\mathfrak{A}$ ein H mit $He' = e$, so ist H ein Automorphismus, und es liegt auch H^{-1} in $\mathfrak{A}$. Die Menge aller Automorphismen $A \in \mathfrak{A}$ bildet die größte Untergruppe von $\mathfrak{A}$ mit Einselement E.*

b) *$\mathfrak{A}$ ist dann und nur dann auch e'-einfach-transitiv, wenn der Endomorphismus $H \in \mathfrak{A}$ mit $He = e'$ ein Automorphismus ist.*

Beweis. a) Mit $H_{a,e}$ bezeichnen wir allgemein den eindeutigen Endomorphismus H aus $\mathfrak{A}$, für den $H_{a,e}e = a$. Ist nun $H \in \mathfrak{A}$ und $He' = e$, so haben wir $(H \cdot H_{e',e})e = e = Ee$ und damit $H \cdot H_{e',e} = E$; wegen der Kommutativität von $\mathfrak{A}$ gilt aber auch $H_{e',e} \cdot H = E$. Aus diesen beiden Gleichungen folgt aber bekanntlich: $H = A$ ist ein Automorphismus, und es ist $H_{e',e} = A^{-1}$. — Der Rest von a) ist trivial, ebenso ist b) eine triviale Folgerung von a).

SATZ 1. a) *Jede Abelsche e-einfach-transitive Halbgruppe $\mathfrak{A}$ ist ein Endomorphismen-Ring, $\mathfrak{A} = \mathfrak{R}$, und es gilt $H_{a+b,e} = H_{a,e} + H_{b,e}$ $(a, b \in \mathfrak{A})$.*

b) *Führt man in $\mathfrak{A}$ mit Hilfe von $\mathfrak{A}$ eine e-Multiplikation ein durch die Vorschrift $(a \cdot b)_e = (H_{a,e} \cdot H_{b,e})e$, so wird $\mathfrak{A}$ zu einem Ring $\mathfrak{R}_e$ mit Einselement e, der durch die Vorschrift $a \to H_{a,e}$ kanonisch isomorph auf $\mathfrak{R}$ abgebildet wird.*

Beweis. a) Es genügt zu zeigen: Für $a, b \in \mathfrak{A}$ gilt in $\mathfrak{A}$ stets $H_{a,e} + H_{b,e} = H_{a+b,e}$. Nun hat man für beliebige $c \in \mathfrak{A}$: $H_{a+b,e}c = (H_{a+b,e} \cdot H_{c,e})e = H_{c,e}(H_{a+b,e}e) = H_{c,e}(a+b) = H_{c,e}a + H_{c,e}b = (H_{c,e} \cdot H_{a,e})e + (H_{c,e} \cdot H_{b,e})e = H_{a,e}(H_{c,e}e) + H_{b,e}(H_{c,e}e) = H_{a,e}c + H_{b,e}c$. Wegen der Willkürlichkeit von c gilt also $H_{a+b,e} = H_{a,e} + H_{b,e}$. (Für $a = e$, $b = 0$ folgt speziell $H_{e,e} = E = E + H_{0,e}$; $H_{0,e} = N$.) — b) ist im wesentlichen trivial.

Ist $H_{e',e} = A_{e',e} \in \mathfrak{A}$ ein Automorphismus, so ist $\mathfrak{A}$ nach Hilfssatz 2 auch e'-einfach-transitiv, und es wird daher $\mathfrak{A}$ durch Einführung der e'-Multiplikation $(a \cdot b)_{e'} = (H_{a,e'} \cdot H_{b,e'})e'$ zu einem Ring $\mathfrak{R}'_{e'}$ mit Einselement e', der ebenso wie $\mathfrak{R}_e$ zu $\mathfrak{R}$ isomorph ist. Um einen direkten Zusammenhang zwischen $\mathfrak{R}_e$ und $\mathfrak{R}'_{e'}$ herzustellen, müssen wir jedes $H_{a,e}$ aus $\mathfrak{A}$ auf die Form $H_{a',e'}$ bringen, d.h. wir haben $H_{a,e}e'$ zu berechnen. Es ergibt sich: $H_{a,e}e' = (H_{a,e} \cdot A_{e',e})e = A_{e',e}(H_{a,e}e) = A_{e',e}a$, d.h. wir haben die *Umrechnungsformel:*

$$H_{a,e} = H_{A_{e',e}a,e'} \qquad (a \in \mathfrak{A}). \tag{1}$$

Aus der Umrechnungsformel folgt sofort: $A_{e',e}\big((a\cdot b)_e\big)=(A_{e',e}\cdot H_{a,e}\cdot H_{b,e})\,e=(H_{a,e}\cdot H_{b,e})\,(A_{e',e}e)=(H_{a,e}\cdot H_{b,e})\,e'=(H_{A_{e',e}a,e'}\cdot H_{A_{e',e}b,e'})\,e'=(A_{e',e}a\cdot A_{e',e}b)_{e'}$. Aus dieser Bemerkung ergibt sich weiter mühelos:

Satz 2. *Ist $A_{e',e}$ ein Automorphismus aus $\mathfrak{A}$ und $\mathscr{R}_e$ bzw. $\mathscr{R}'_{e'}$ der mit Hilfe von $\mathfrak{A}$ aus $\mathscr{A}$ abgeleitete Ring mit dem Einselement e bzw. e', so bildet $A_{e',e}$ den Ring $\mathscr{R}_e$ ringisomorph auf $\mathscr{R}'_{e'}$ ab.*

Durch Satz 1 und Satz 2 ist gezeigt: *Jede* hinsichtlich eines Elements $e\in\mathscr{A}$ einfach-transitive Abelsche Endomorphismen-Halbgruppe kann benutzt werden, um aus $\mathscr{A}$ einen Ring $\mathscr{R}_e$ zu machen. Im allgemeinen kann mit Hilfe einer Halbgruppe $\mathfrak{A}$ sogar eine ganze Klasse von Ringen gewonnen werden, doch sind alle Ringe einer solchen Klasse kanonisch untereinander isomorph. —

Um den Spezialfall der *Körper* besonders zu würdigen, definieren wir: Eine *Automorphismen-Gruppe* $\mathfrak{G}$ von $\mathscr{A}$ soll *einfach-transitiv* heißen, wenn in $\mathfrak{G}$ für jedes Paar $a\neq 0$, $b\neq 0$ aus $\mathscr{A}$ genau ein Automorphismus A mit $Aa=b$ existiert. Natürlich ist $\mathfrak{G}$ bereits dann einfach-transitiv, wenn die angegebene Bedingung für alle Paare $e=a, b$ mit festem e erfüllt ist. Ist $\mathfrak{G}$ eine einfach-transitive Automorphismen-Gruppe, so ist $\mathfrak{G}\cup\{N\}$ für jedes $e\neq 0$ aus $\mathscr{A}$ eine e-einfach-transitive Endomorphismen-Halbgruppe im bisherigen Sinne. Aus dieser Bemerkung, Hilfssatz 2 und Satz 1a) folgt fast unmittelbar:

Satz 3. *Die Menge aller der e-einfach-transitiven Abelschen Endomorphismen-Halbgruppen $\mathfrak{A}$, die gleichzeitig Endomorphismen-Körper sind, wird durch die Vorschrift $\mathfrak{A}\to\mathfrak{A}-\{N\}$ umkehrbar eindeutig auf die Menge aller einfach-transitiven Abelschen Automorphismen-Gruppen $\mathfrak{G}$ abgebildet.*

Um also alle Möglichkeiten zu übersehen, wie $\mathscr{A}$ zu einem *Körper* gemacht werden kann, hat man sich nur einen Überblick über die Menge aller einfach-transitiven Abelschen Automorphismen-Gruppen $\mathfrak{G}$ zu verschaffen.

Fragen wir nach den Schwierigkeiten, auf die man stößt, wenn man die gewonnenen Resultate auf Schiefringe übertragen will, so lautet die Antwort so: Ist $\mathfrak{C}$ eine beliebige e-einfach-transitive Endomorphismen-Halbgruppe, und versucht man, in $\mathscr{A}$ eine e-Multiplikation durch $(a\cdot b)_e=(H_{a,e}\cdot H_{b,e})e$ einzuführen, so zeigt sich, daß zwar die Assoziativität der Multiplikation und das distributive Gesetz $\big(c\cdot(a+b)\big)_e=(c\cdot a)_e+(c\cdot b)_e$ sofort verifiziert werden können, daß aber die Gültigkeit des distributiven Gesetzes $\big((a+b)\cdot c\big)_e=(a\cdot c)_e+(b\cdot c)_e$ gleichwertig ist mit der Allgemeingültigkeit der Gleichung $H_{a+b,e}=H_{a,e}+H_{b,e}$, die in Satz 1a) nur unter scharfer Ausnutzung der Kommutativität bewiesen werden konnte. — Setzt man ferner für $\mathfrak{C}$ die Gültigkeit von $H_{a+b,e}=H_{a,e}+H_{b,e}$ voraus, und ist $A_{e',e}$ ein in $\mathfrak{C}$ enthaltener Automorphismus, so wird zwar $\mathscr{A}$ durch die Multiplikationsdefinition $(a\cdot b)_e=(H_{a,e}\cdot H_{b,e})e$ bzw. $(a\cdot b)_{e'}=(H_{a,e'}\cdot H_{b,e'})e'$ jeweils zu einem Schiefring $\mathscr{R}_e$ bzw. $\mathscr{R}'_{e'}$ mit dem Einselement e bzw. e'. Aber es ist zum mindesten nicht selbstverständlich, daß der Gruppen-Automorphismus $A_{e',e}$ den Schiefring $\mathscr{R}_e$ isomorph auf $\mathscr{R}'_{e'}$ abbildet. Denn beim Beweis der Umrechnungsformel (1) wurde wieder wesentlich die Kommutativität von $\mathfrak{A}$ ausgenützt.

§ 2. Total geordnete Archimedische Abelsche Gruppen

Es sei jetzt die Abelsche Gruppe $\mathscr{A}$ total geordnet. $\mathscr{H}$ sei die Unterhalbgruppe aller echt positiven Elemente. $\mathscr{A}$ sei Archimedisch, es gebe also zu jedem Paar $a, b \in \mathscr{H}$ ein n, derart daß $n \cdot a > b$. Betrachtet wird die Halbgruppe $\mathfrak{E}^*$ aller der Endomorphismen H von $\mathscr{A}$, die entweder die Ordnung von $\mathscr{A}$ erhalten (d.h. $a > b \Rightarrow Ha > Hb$) oder sie umkehren ($a > b \Rightarrow Ha < Hb$). $\mathfrak{E}$ sei die Unterhalbgruppe aller ordnungserhaltenden Endomorphismen, mit $-E$ werde der durch $(-E)a = -a$ festgelegte, zu $\mathfrak{E}^*$ aber nicht zu $\mathfrak{E}$ gehörige Automorphismus bezeichnet. Dann wissen wir: Es ist $\mathfrak{E}^* = \mathfrak{E} \cup (-E) \cdot \mathfrak{E}$, und es gilt $(-E) \cdot H = H \cdot (-E)$ für alle $H \in \mathfrak{E}^*$. Gibt es genau einen Endomorphismus $H \in \mathfrak{E}^*$ mit $Ha = b$, so gibt es auch genau einen Endomorphismus $H' \in \mathfrak{E}^*$ mit $H'a = -b$, nämlich $H' = (-E) \cdot H$. Nennen wir ferner für $e \in \mathscr{H}$ die Unterhalbgruppe $\mathfrak{C}$ von $\mathfrak{E}$ e-einfach-transitiv *in* $\mathscr{H}$, wenn zu jedem $a \in \mathscr{H}$ ein $H \in \mathfrak{C}$ mit $He = a$ existiert, so sieht man sofort: Eine Unterhalbgruppe $\mathfrak{C}^*$ von $\mathfrak{E}^*$ ist dann und nur dann e-einfach-transitiv, wenn $\mathfrak{C} = \mathfrak{C}^* \cap \mathfrak{E}$ e-einfach-transitiv in $\mathscr{H}$ ist. $\mathfrak{C}^*$ ist dann und nur dann e-einfach-transitiv, wenn $\mathfrak{C}^*$ $(-e)$-einfach-transitiv ist. Diese Bemerkungen gestatten es, im folgenden zunächst nur $\mathfrak{E}$ zu betrachten, und da jeder $H \in \mathfrak{E}$ einen Endomorphismus von $\mathscr{H}$ induziert, durch den er selbst eindeutig bestimmt ist, dürfen und wollen wir dabei die $H \in \mathfrak{E}$ geradezu mit den induzierten Endomorphismen von $\mathscr{H}$ identifizieren. In der späteren Formulierung der Hauptsätze können wir dann ohne neue Sonderbetrachtungen die gewonnenen Ergebnisse unmittelbar für $\mathfrak{E}^*$ und $\mathscr{A}$ formulieren.

Zunächst definieren wir im Sinne des 5. Buches von Euklid: Es seien $a, b, c, d \in \mathscr{H}$; das Paar $\langle a, b \rangle$ soll *proportional* zu $\langle c, d \rangle$ heißen, wenn für alle natürlichen Zahlen m, n gilt:

$$(2) \qquad \begin{cases} m \cdot a > n \cdot b \Rightarrow m \cdot c > n \cdot d \\ m \cdot a = n \cdot b \Rightarrow m \cdot c = n \cdot d \\ m \cdot a < n \cdot b \Rightarrow m \cdot c < n \cdot d. \end{cases}$$

Ersichtlich ist die Proportionalität eine Äquivalenzrelation. Bezeichnet $a:b$ die Klasse aller zu $\langle a, b \rangle$ proportionalen Paare, so können wir kurz $a:b = c:d$ schreiben, falls (2) erfüllt ist. Offenbar folgt aus $a:b = c:d$ stets $b:a = d:c$, und es gilt das

1. ADDITIONSGESETZ: $a:b = c_1:d_1 = c_2:d_2 \Rightarrow a:b = (c_1 + c_2):(d_1 + d_2)$.

Im Anschluß an Euklid beweisen wir jetzt drei fundamentale Hilfssätze.

HILFSSATZ 3. *Aus* $a:b = a:b'$ *folgt stets* $b = b'$.

Beweis indirekt. Es sei etwa $b' = b + e > b$. Dann gibt es m, n derart, daß $m \cdot b > a$, $m \cdot e > a$, $n \cdot a \leqq m \cdot b < (n+1) \cdot a$, und weiter folgt $(n+1) \cdot a \leqq m \cdot b + a < m \cdot b + m \cdot e = m \cdot b'$. Es ist also sicher $a:b \neq a:b'$.

HILFSSATZ 4. *Aus* $a:b = c:d$ *und* $a > c$ *folgt stets* $b > d$.

Beweis indirekt. Angenommen es sei $b \not> d$; dann ist $d = b + e > b$, denn aus $d = b$ folgte $a = c$ nach Hilfssatz 3. Es gibt nun m, n derart, daß $m \cdot b > a$,

$m \cdot e > a$, $n \cdot a \leqq m \cdot b < (n+1) \cdot a$, und man erhält: $(n+1) \cdot c < n \cdot a + a < m \cdot b + m \cdot e = m \cdot d$; $a:b \neq c:d$.

Hilfssatz 5. *Aus $a:b = c:d$ folgt stets $a:c = b:d$.*

Zunächst nämlich folgt aus $a:b = c:d$ trivialerweise $(m \cdot a):(m \cdot b) = (n \cdot c):(n \cdot d)$ für jedes Paar m, n. Nach Hilfssatz 3 und Hilfssatz 4 ergibt sich weiter: Aus $m \cdot a >$ bzw. $=$ bzw. $< n \cdot c$ folgt $n \cdot b >$ bzw. $=$ bzw. $< n \cdot d$; d.h. es gilt (2) für die Paare $\langle a, c\rangle$, $\langle b, d\rangle$.

Wendet man auf das erste Additionsgesetz Hilfssatz 5 an, so ergibt sich das

2. Additionsgesetz: $a:b_1 = c:d_1$, $a:b_2 = c:d_2 \Rightarrow a:(b_1 + b_2) = c:(d_1 + d_2)$.

Den Ausgangspunkt für die Endomorphismen-Theorie von $\mathscr{H}$ liefert das folgende Lemma, das unmittelbar aus der Definition der ordnungserhaltenden Endomorphismen folgt.

Lemma. *Für beliebige $a, b \in \mathscr{H}$ und $H \in \mathfrak{E}$ gilt $a:b = Ha:Hb$.*

Wenden wir die Hilfssätze 3, 4, 5 auf die Endomorphismen-Theorie von $\mathscr{H}$ an, so erhalten wir die folgenden Sätze, die wir aus den zu Beginn des Paragraphen angegebenen Gründen gleich für $\mathfrak{E}^*$ und $\mathscr{A}$ formulieren können.

Satz 4. *Ein Endomorphismus $H \in \mathfrak{E}^*$ von $\mathscr{A}$ ist durch Angabe eines einzigen Urbild-Bild-Paares $\langle a, Ha = c\rangle$ eindeutig bestimmt. — Jeder Endomorphismus H ist ein Endo-Isomorphismus.*

Triviale Folge aus dem Lemma und Hilfssatz 3 (für die Endomorphismen von $\mathscr{H}$).

Für beliebige $e \in \mathscr{A}$ erhalten wir als

Korollar. *Ist $\mathfrak{E}^*$ e-transitiv, so ist $\mathfrak{E}^*$ sogar e-einfach-transitiv.*
Ist $\mathfrak{C}^* \leqq \mathfrak{E}^*$ und $\mathfrak{C}^*$ e-transitiv, so ist $\mathfrak{C}^* = \mathfrak{E}^*$.

Satz 5. *Jeder Endomorphismus $H \in \mathfrak{E}$ ist ordnungsmonoton im folgenden Sinne: Gilt bei einem Urbild-Bild-Paar $\langle a, Ha\rangle$ die Beziehung $Ha > a$ bzw. $Ha < a$, so gilt sie bei allen Urbild-Bild-Paaren.*

Triviale Folgerung aus dem Lemma und Hilfssatz 4. — Man beachte, daß diesmal die Formulierung umständlicher würde, wenn wir von $\mathscr{H}$, $\mathfrak{E}$ zu $\mathscr{A}$, $\mathfrak{E}^*$ übergehen wollten. Satz 5 ist vor allem deshalb wichtig, weil er die tiefere Bedeutung von Hilfssatz 4 zeigt, aus dem wir Hilfssatz 5 ableiteten. Hilfssatz 5 seinerseits führt rasch zu dem entscheidenden Theorem:

Satz 6. *Die Endomorphismen-Halbgruppe $\mathfrak{E}^*$ ist kommutativ.*

Beim Beweis drücken wir, gestützt auf Satz 4, analog wie in § 1 durch die Schreibweise $H = H_{b,a}$ die Tatsache aus, daß H der (einzige) Endomorphismus mit $Ha = b$ ist. Es seien $H, Z \in \mathfrak{E}$; $a \in \mathscr{H}$ und $Z = H_{c,a}$, $H = H_{d,c} = H_{b,a}$. Dann haben wir $H \cdot Z = H_{d,a}$, und wegen $Z \cdot H = H_{c,a} \cdot H_{b,a}$ bleibt nur $H_{c,a} = H_{d,b}$ zu beweisen. Nun ist $a:c = b:d$ wegen $H = H_{d,c} = H_{b,a}$, und $a:b = c:d$, $H_{c,a} = H_{d,b}$ folgt aus Hilfssatz 5.

Satz 6 liefert in Verbindung mit Satz 1a) unmittelbar:

SATZ 7. *Ist* $\mathfrak{E}^*$ *hinsichtlich irgendeines Elementes* e *transitiv, so ist* $\mathfrak{E}^*$ *ein (kommutativer) Ring, in dem allgemein die Formel* $H_{a+b,e}=H_{a,e}+H_{b,e}$ *gilt, und man kann — mit* $\mathfrak{E}^*$ *statt* $\mathfrak{A}$ *— die Sätze* 1, 2, 3 *von* § 1 *auf* $\mathscr{A}$ *anwenden.*

Zusatz. $\mathfrak{E}^*$ *ist als Ring stets nullteilerfrei, und zwar von Charakteristik* 0. (Klar, da alle Endomorphismen nach Satz 4 Endo-Isomorphismen sind, und aus $H \neq N$ stets $n \cdot H \neq N$ folgt.)

Fragen wir nach einer einfachen Bedingung dafür, daß $\mathfrak{E}^*$ hinsichtlich des Elementes e, das nach früheren Bemerkungen positiv angenommen werden darf, transitiv ist, so kommen wir zu folgendem Theorem, das nochmals zu den Proportionen zurückführt.

SATZ 8. $\mathfrak{E}^*$ *ist dann und nur dann hinsichtlich* $e \in \mathscr{H}$ *transitiv, wenn zu jedem Tripel* e, b, c *aus* $\mathscr{H}$ *in* $\mathscr{H}$ *die „vierte Proportionale", d.h. ein (notwendig eindeutiges)* d *mit* $e:b=c:d$ *existiert.*

Beweis. Ist $H=H_{c,e}$ und $b \in \mathscr{H}$ beliebig, so genügt $d=Hb$ nach dem Lemma der Bedingung $e:b=c:d$, unsere Voraussetzung ist also notwendig. Ist sie andererseits erfüllt, so definiert die Vorschrift „$Hb=d$, wenn $e:b=c:d$" jedenfalls eine ordnungserhaltende Abbildung von $\mathscr{H}$ in $\mathscr{H}$. Aus dem 2. Additionsgesetz (mit e statt a) folgt aber sofort, daß die von uns definierte Abbildung H der Bedingung $H(b_1+b_2)=Hb_1+Hb_2$ genügt, also ein Endomorphismus (von $\mathscr{H}$ und damit nach Erweiterung auf $\mathscr{A}$ auch ein solcher von $\mathscr{A}$) ist.

Besonders hervorzuheben ist, daß wir uns beim Beweise von Satz 8 auf Hilfssatz 5 stützen mußten. Satz 8 ist also keine Trivialität, wie man auf den ersten Blick meinen könnte. Ziehen wir die Resultate von § 1 heran, so ergibt sich fast unmittelbar:

KOROLLAR ZU SATZ 8. $\mathfrak{E}^*$ *ist genau dann e-transitiv (für geeignetes* $e \in \mathscr{H}$*) und ein Körper, wenn in* $\mathscr{H}$ *immer — d.h. zu jedem Tripel* a, b, c *— die durch* $a:b=c:d$ *charakterisierte vierte Proportionale* d *existiert.*

In diesem Falle ist $\mathfrak{E}^*$ *sogar a-einfach-transitiv für alle* $a \in \mathscr{H}$.

Die letzte Behauptung folgt unmittelbar aus dem Korollar zu Satz 4 und Hilfssatz 2.

Die Möglichkeit, daß $\mathfrak{E}^*$ zwar ein Körper, aber hinsichtlich keines einzigen a transitiv ist, also sozusagen ein „zu kleiner" Körper ist, soll hier nicht weiter diskutiert werden. — Wir bemerken schließlich noch:

SATZ 9. *Ist* $\mathfrak{E}^*$ *e-transitiv für ein* $e \in \mathscr{H}$, *so wird* $\mathfrak{E}^*$ *zu einem total geordneten Archimedischen Ring mit zu* $\mathscr{A}$ *ordnungsisomorpher Additionsgruppe, wenn man festsetzt:* $H=H_{a,e}>N=H_{0,e}$ *dann und nur dann, wenn* $a>0$.

Zum Beweis hat man nur zu beachten: a) Wegen $H_{a,e}+H_{b,e}=H_{a+b,e}$ wird $\mathfrak{E}^*$ als Additionsgruppe durch die Vorschrift $H_{a,e} \leftrightarrow a$ ordnungsisomorph auf $\mathscr{A}$ abgebildet. — b) Ist $H=H_{a,e}>Z=H_{b,e}$, also $a>b$, und $Z'=H_{c,e}>N$, also $c>0$, so hat man $H_{a,e}-H_{b,e}=H_{a-b,e}$, $a-b>0$, und daraus folgt $H_{c,e}\cdot(H_{a,e}-H_{b,e})=H_{d,e}>N=H_{0,e}$; denn es ist $d>0$, weil $H_{c,e}$ und $H_{a,e}-H_{b,e}=H_{a-b,e}$ beide zu $\mathfrak{E}$ gehören und $e \in \mathscr{H}$ ist.

Wieder verzichten wir auf die Untersuchung der Frage, welche Ordnungsaussagen gemacht werden können, wenn $\mathfrak{E}^*$ hinsichtlich keines einzigen Elementes transitiv ist.

§ 3. Historische und didaktische Bemerkungen

Wollen wir auf Grund von § 1 und § 2 die Bedeutung des 5. Buches Euklids vom modernen Standpunkt würdigen, so ist einerseits die zentrale Stellung der Hilfssätze 3—5 in § 2 zu beachten; andererseits ist zu berücksichtigen, daß die vierte Proportionale im Werk Euklids eine fundamentale Rolle spielt und daß, wie in einer im Rohentwurf bereits vorliegenden Dissertation unter anderem gezeigt werden soll, tatsächlich sogar im 5. Buch die Existenz der vierten Proportionalen an mindestens einer Stelle stillschweigend vorausgesetzt wird. Wir wollen daher angesichts der Tatsache, daß das 5. Buch Euklids inhaltlich auf Eudoxos zurückgeht, eine total geordnete Archimedische Abelsche Gruppe $\mathscr{A}$ kurz als *Eudoxische Gruppe* bezeichnen, wenn in $\mathscr{A}$ zu jedem positiven Tripel a, b, c die vierte Proportionale existiert.

Um einen möglichst engen Anschluß an die Griechen zu gewinnen, definieren wir weiter: Unter einer Eudoxischen Halbgruppe $\mathscr{H}$ bzw. einem total geordneten Halbkörper $\mathfrak{L}$ soll die Menge aller positiven Elemente einer Eudoxischen Gruppe $\mathscr{A}$ bzw. eines total geordneten Körpers $\mathfrak{K}$ verstanden werden. Man sieht dann sofort: Eudoxische Halbgruppen und total geordnete Halbkörper können genausogut selbständig axiomatisch eingeführt werden wie die entsprechenden Gruppen und Körper. Der einzige Unterschied ist der, daß man bei der Addition die Forderung: „Zu jedem Paar a, b gibt es ein c mit $a+c=b$" ersetzen muß durch die Forderung: „Zu a, b gibt es dann und nur dann ein c mit $a+c=b$, wenn $b>a$." — Weiter überzeugt man sich mühelos, daß jede Eudoxische Halbgruppe $\mathscr{H}$ bzw. jeder total geordnete Halbkörper $\mathfrak{L}$ sofort zu einer Eudoxischen Gruppe $\mathscr{A}$ bzw. einem total geordneten Körper $\mathfrak{K}$ erweitert werden kann, derart daß $\mathscr{H}$ bzw. $\mathfrak{L}$ gerade die Menge aller positiven Elemente von $\mathscr{A}$ bzw. $\mathfrak{K}$ darstellt. Es ist also auch vom axiomatischen Standpunkt aus ganz unwesentlich, wenn wir — den Griechen folgend, die weder eine Null noch negative Elemente kannten — mit Halbgruppen und Halbkörpern statt mit Gruppen und Körpern operieren. Dann aber zeigt eine Überprüfung der Schlüsse von § 1 und § 2:

Der Satz: „*Bei jeder Eudoxischen Halbgruppe $\mathscr{H}$ bildet die Menge aller ordnungserhaltenden Automorphismen einen total geordneten Halbkörper $\mathfrak{L}$, der als additive Halbgruppe zu $\mathscr{H}$ kanonisch ordnungsisomorph ist*", folgt so rasch und einfach aus den klassischen Hilfssätzen 3, 4, 5, daß mit Recht behauptet werden kann: Der genannte Satz ist für den aufmerksamen Leser bereits im 5. Buch Euklids zu finden, vorausgesetzt allerdings, daß dieser Leser mit dem modernen, den Griechen noch fremden Automorphiebegriff vertraut ist.

Zum Beweis beachte man: Man braucht, um den fraglichen Satz aus den Hilfssätzen 3, 4, 5 abzuleiten, zunächst (nur für Automorphismen) den trivialen Satz 4 von § 2, sowie Satz 6, dessen durch eine kurze Automorphismenrechnung

geführter Beweis allerdings etwas aus dem klassischen griechischen Rahmen herausfällt. Dann ist (entsprechend dem Hauptteil des Beweises von Satz 8) zu zeigen: Sind a, c gegeben und definiert man allgemein: „$Ab=d$, falls $a:b=c:d$", so entsteht ein Automorphismus A von $\mathfrak{H}$. Im Fall einer Eudoxischen Halbgruppe ist nun von vornherein klar, daß A eine Abbildung von $\mathfrak{H}$ *auf* $\mathfrak{H}$ darstellt. (Ist d gegeben, so wird $Ab=d$, falls $a:b=c:d$.) Es bleibt $A(b_1+b_2)=Ab_1+Ab_2$ zu beweisen, und das geschieht, wie in § 2 bei Satz 8, ganz in klassisch griechischer Weise durch Herleitung des 2. Additionsgesetzes aus dem ersten. Schließlich brauchen wir noch die Formel $A_{a+b,c}=A_{a,c}+A_{b,c}$. Hier treten wir wieder aus dem engeren griechischen Rahmen, denn wir müssen auf Satz 1a) von § 1 zurückgreifen. Aber es ist wenigstens auch hier die zum Beweis nötige Rechnung außerordentlich kurz und elementar.

Auf jeden Fall zeigt unsere Analyse: Es ist auch heute noch durchaus nicht abwegig, zu überlegen, wie sich der Aufbau der Analysis gestaltet, wenn man soweit wie möglich dem Vorbild der Griechen folgt, für die es (bei den uns interessierenden Fragen) nur ganze Zahlen und „Größen", aber jedenfalls keine reellen Zahlen gab. Die „Größen", mit denen sich die Griechen beschäftigten, waren durchweg der Geometrie entnommen. Nichts hindert uns aber, auch Beispiele aus der Physik heranzuziehen: Die Betrachtung geometrischer und physikalischer Größen und der dort auftretenden Additivität führt durch Abstraktion zwanglos zum Begriff der total geordneten Abelschen Gruppe. (Wir werden im Gegensatz zu den Griechen nicht bei der Halbgruppe stehenbleiben, da in der Physik auch negative Größen auftreten.) Die Plausibilität des Archimedischen Axioms ist leicht an Beispielen klarzumachen. Es fragt sich nur, wie es in dieser Hinsicht mit dem Zusatzaxiom steht, durch das wir die Eudoxischen Gruppen gekennzeichnet hatten. Hier ist anzuknüpfen an die Vorstellung, daß man Größen durch Vergleich mit einer Maßgröße erfaßt, daß aber in einem „homogenen" Größensystem die spezielle Wahl der Maßgröße gleichgültig sein muß. Diese Überlegung führt durch Abstraktion zur Auszeichnung derjenigen total geordneten Abelschen Gruppen, bei denen zu $a\neq 0$, $c\neq 0$ stets ein Automorphismus A mit $Aa=c$ existiert. Bei dem Versuch, derartige Gruppen näher zu charakterisieren, kommt man schließlich, wie in § 2 gezeigt, zwanglos zum Proportionalitätsbegriff und zur axiomatischen Einführung der Eudoxischen Gruppen. Das heißt also: Sieht man es als eine Grundaufgabe der Mathematik an, eine Theorie zu entwickeln, die als Grundlage für die Behandlung geometrischer und physikalischer Größensysteme dienen kann, so ist es durchaus plausibel, eine systematische Untersuchung der Eudoxischen Gruppen an den Anfang zu stellen. Von diesem Ausgangspunkt kommt man dann, wie gezeigt, zwangsläufig zur Einführung des Körperbegriffs, und zwar tragen die auftretenden Körper wegen ihrer Archimedischen Totalordnung „reellen" Charakter. Es wäre also ein Irrtum, anzunehmen, der „griechische" Grundsatz, nach der Einführung der ganzen Zahlen sich zunächst auf die Betrachtung von Größensystemen zu beschränken, sperre den Zugang zum Körperbegriff. Nur sind die Elemente der auf dem „griechischen" Weg gewonnenen Körper nicht rationale oder reelle „Zahlen",

sondern Automorphismen. Im übrigen bleibt man bis zur Konstruktion der Automorphismen-Körper einschließlich durchaus im Algebraischen. Die Untersuchungen erfordern nirgends die Einführung eines Begriffs wie des der Menge aller Dedekindschen Schnitte — obwohl bekanntlich DEDEKIND mit seiner Schnittdefinition bewußt an das 5. Buch Euklids anknüpfte. Auf die Bedeutung dieser Erkenntnis für die Würdigung des 5. Buches vom modernen Standpunkt sei hier nur andeutungsweise hingewiesen.

Hingegen sei kurz ausgeführt, wie nach dem systematischen algebraischen Studium der Eudoxischen Gruppen zwanglos der Anschluß an die übliche, auf dem Begriff des reellen Zahlkörpers aufbauende Analysis gewonnen werden kann. Man geht am besten aus von der Betrachtung „mehrdimensionaler" Größensysteme, wie sie in der Physik auftreten. Hier sind zunächst mehrere total geordnete Archimedische Gruppen $\mathfrak{A}_i$ gegeben, und um rechnerisch weiterzukommen, muß man die $\mathfrak{A}_i$ alle in eine gemeinsame Obergruppe des gleichen Typus (ordnungsisomorph) einbetten. In diesem Zusammenhang liegt aber die Frage nach einer *Universalgruppe* $\mathfrak{A}_u$, in die *jede* total geordnete Archimedische Gruppe einbettbar ist, sehr nahe. Man wird sie also aufgreifen und folgendermaßen beantworten: Bildet man zu einer beliebigen, nichtdiskreten, total geordneten Archimedischen Gruppe $\mathfrak{A}$ in üblicher Weise die vollständige Hülle $\mathfrak{A}_u$ hinsichtlich der Ordnungstopologie von $\mathfrak{A}$, so ist $\mathfrak{A}_u$ eine Universalgruppe in dem von uns gewünschten Sinne. $\mathfrak{A}_u$ ist, unabhängig von der speziellen Wahl der Ausgangsgruppe $\mathfrak{A}$, bis auf Ordnungsisomorphie eindeutig bestimmt, so daß man unbedenklich von *der* Universalgruppe sprechen darf, die zur Menge aller total geordneten Archimedischen Gruppen gehört. — Weiter zeigt man mühelos, daß $\mathfrak{A}_u$ Eudoxisch ist, daß also der zu $\mathfrak{A}_u$ gehörige Endomorphismenring $\mathfrak{E}_u^* = \mathfrak{K}_u^*$ ein total geordneter Archimedischer Körper ist, in dem die Endomorphismenkörper aller Eudoxischen Gruppen ordnungsisomorph eingebettet werden können. Da nun $\mathfrak{K}_u^*$ mühelos mit dem Körper aller reellen Zahlen identifiziert werden kann, haben wir so den Anschluß an die üblichen Grundlagen der Analysis gewonnen.

Bei unserem Aufbau wird man allerdings fragen, ob ein so früher Übergang zur Universalgruppe $\mathfrak{A}_u$ tatsächlich sinngemäß ist. Sollte man nicht die Heranziehung des topologischen Begriffs der vollständigen Hülle auf einen späteren Zeitpunkt verschieben und zunächst noch weiter rein algebraisch vorgehen? Hier darf nicht verschwiegen werden, daß der Versuch einer ausschließlich algebraischen Weiterentwicklung der Theorie der total geordneten Archimedischen Gruppen rasch auf überraschende Schwierigkeiten führt. Zunächst hatten wir uns ja auf das Studium der in plausibler Weise axiomatisch charakterisierten *Eudoxischen* Gruppen beschränkt. Darüberhinaus aber wird man die Frage nach expliziten Beispielen nichttrivialer Eudoxischer Gruppen nicht umgehen können — wobei die leicht einzuführende Additionsgruppe der rationalen Zahlen wohl als trivial anzusehen ist. Nun sind aber die einfachsten Beispiele total geordneter Archimedischer Gruppen (etwa Gruppen mit endlich vielen, paarweise inkommensurablen Erzeugenden) alle nicht-Eudoxisch; man stößt daher zwangsläufig auf das folgende Problem: Es soll eine beliebig

vorgegebene Archimedische Gruppe $\mathfrak{A}$ durch einen möglichst einfachen algebraischen Prozeß (etwa entsprechend dem Übergang von einem Integritätsbereich zu seinem Quotientenkörper) in eine kleinste umfassende Eudoxische Gruppe $\mathfrak{A}_e$ eingebettet werden. Was diese Aufgabe angeht, so zeigen die Untersuchungen von § 2: Die Lösung ist leicht, wenn die Gruppe $\mathfrak{A}$ hinsichtlich irgendeines e transitiv ist. Denn in diesem Falle läßt sich die Einbettung von $\mathfrak{A}$ in $\mathfrak{A}_e$ zurückführen auf die Einbettung des zugehörigen Endomorphismen-Ringes $\mathfrak{E}^*$ in seinen Quotientenkörper. Im allgemeinen ist aber der Endomorphismen-Ring $\mathfrak{E}^*$ von $\mathfrak{A}$, kurz gesagt „zu klein". Ist z.B. $\mathfrak{E}^*$ isomorph zum Ring der ganzen rationalen Zahlen, was unter anderem bei weitaus den meisten durch zwei inkommensurable Elemente erzeugten Gruppen $\mathfrak{A}$ zutrifft, so entspricht dem Übergang von $\mathfrak{E}^*$ zu seinem Quotientenkörper nur der Übergang von $\mathfrak{A}$ zur kleinsten Divisionsobergruppe, d.h. zur kleinsten Obergruppe $\mathfrak{A}_b$, in der zu jedem Paar n, a ein b mit $n \cdot b = a$ existiert. Im allgemeinen, insbesondere bei den erwähnten von zwei inkommensurablen Elementen erzeugten Gruppen, ist aber $\mathfrak{A}_b$ keineswegs Eudoxisch.

Die Betrachtung von solchen und ähnlichen Beispielen zeigt: Die Frage, wie weit eine gegebene total geordnete Archimedische Additionsgruppe $\mathfrak{A}$ eine ausgezeichnete multiplikative Struktur besitzt und wie $\mathfrak{A}$ rein algebraisch in eine möglichst kleine Obergruppe eingebettet werden kann, die vom multiplikativen Standpunkt aus ideal, d.h. Eudoxisch ist — diese Frage führt auf weit kompliziertere Probleme, als man bei oberflächlicher Betrachtung annehmen möchte. Man wird sich daher mit ihr nur dann näher beschäftigen, wenn eine systematische Untersuchung der total geordneten Archimedischen Gruppen von allen möglichen Gesichtspunkten aus beabsichtigt ist. Handelt es sich dagegen nur um einen Aufbau der Grundlagen der Analysis, der nach griechischem Vorbild das Studium von allgemeinen Größensystemen an die Spitze stellt, so ist unbedingt empfehlenswert, die rein algebraischen Untersuchungen nicht allzu weit zu treiben und, wie oben skizziert, durch Einführung des Begriffs der Universalstruktur sowie des topologischen Vollständigkeitsbegriffs verhältnismäßig früh den Anschluß an die klassische Analysis herzustellen, bei der der Körper *aller* reellen Zahlen oder, was auf dasselbe herauskommt, die Universalgruppe $\mathfrak{A}_u$ von vornherein im Mittelpunkt der Betrachtung steht.

Bonn, Mathematisches Institut der Universität

(Eingegangen am 9. April 1960)

Soeben erschienener Nachdruck:

Mathematische Zeitschrift

Band 1 – 50 Heft 1. Berlin, 1918 – 1944	broschiert DM 3600,–
Einzeln: Band 1 – 23, 1918 – 1925	je DM 48,–
Band 24 – 49, 1926 – 1944	je DM 96,–
Band 50 Heft 1, 1944	DM 20,–

Nach dem Kriege, seit 1947 erschienen:

Band 51, 1947 – 1949	DM 112,40
Band 52, 1949 – 1950	DM 163,80
Band 53 – 72, 1950 – 1960	je DM 96,–

Lange & Springer · Wissenschaftliche Buchhandlung

Berlin-Wilmersdorf · Heidelberger Platz 3

Boolean Algebras

By Dr. ROMAN SIKORSKI

(Ergebnisse der Mathematik und ihrer Grenzgebiete
Neue Folge, Heft 25)
In englischer Sprache. IX, 176 Seiten Gr.-8°. 1960. Steif geheftet DM 39,60

FOR INFORMATION

This monograph contains a systematic study of Boolean algebras. Only a knowledge of fundamental notions of General Set Theory and Settheoretical Topology is necessary to understand the book, which is written in an elementary way. Chapter I is devoted to an examination of Boolean algebras from the point of view of finite Boolean operations only. Chapter II is the main part of the book. It is the first systematic exposition of infinite Boolean operations in the mathematical literature. The representation problem for Boolean algebras is the central point of investigation. Both chapters are illustrated by many examples. The Appendix is devoted mainly to applications of Boolean algebras to various branches of mathematics. The book is completed by a long list of papers concerning Boolean algebras.

SPRINGER-VERLAG · BERLIN · GÖTTINGEN · HEIDELBERG

The numerical treatment of differential equations

By Dr. LOTHAR COLLATZ, o. Professor in the University of Hamburg

Third edition

translated from a supplemented version of the second German edition by P. G. WILLIAMS, B. SC., Mathematics Division, National Physical Laboratory, Teddington / England

(Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete. Band 60)

Mit 118 Diagrammen und 1 Porträt. XV, 568 Seiten Gr.-8°. 1960.
In englischer Sprache. DM 93,60; Ganzleinen DM 98,—

CONTENTS

Mathematical preliminaries and some general principles: Introduction to problems involving differential equations. Finite differences and interpolation formulae. Further useful formulae from analysis. Some error distribution principles. Some useful results from functional analysis · Initial-value problems in ordinary differential equations: Introduction. The Runge-Kutta method for differential equations of the n-th order. Finite-difference methods for differential equations of the first order. Theory of the finite-difference methods. Finite-difference methods for differential equations of higher order · Boundary-value problems in ordinary differential equations: The ordinary finite-difference method. Refinements of the ordinary finite-difference method. Some theoretical aspects of the finite-difference methods. Some general methods. RITZ's method for second-order boundary-value problems. RITZ's method for boundary-value problems of higher order. Series solutions. Some special methods for eigenvalue problems · Initial- and initial-/boundary-value problems in partial differential equations: The ordinary finite-difference method. Refinements of the finite-difference method. Some theoretical aspects of the finite-difference methods. Partial differential equations of the first order in one dependent variable. The method of characteristics for systems of two differential equations of the first order. Supplements · Boundary-value problems in partial differential equations: The ordinary finite-difference method. Refinements of the finite-difference method. The boundary-maximum theorem and the bracketing of solutions. Some general methods. The RITZ method. The TREFFTZ method · Integral and functional equations: General methods for integral equations. Some special methods for linear integral equations. Singular integral equations. Volterra integral equations. Functional equations · Appendix · Author index · Subject index.

SPRINGER-VERLAG · BERLIN · GÖTTINGEN · HEIDELBERG